Group Policy Infrastructure

Microsoft Corporation
Published: April 2003
Updated: November 2004

Abstract

Administrators use Group Policy to specify 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. Intended for system administrators, architects, and others who need to create and manage Group Policy settings, this paper explains Group Policy infrastructure and shows how Group Policy Management Console (GPMC), a new MMC snap-in with scripting interfaces, fits into this infrastructure. The paper includes detailed information about Group Policy processing as well as many best practices useful to the Group Policy administrator.

Contents

Introduction

Intended for system administrators, architects, and others who need to create and manage Group Policy settings, this paper explains Group Policy infrastructure and shows how the new Group Policy Management Console (GPMC) fits into this infrastructure. The paper includes detailed information about Group Policy processing as well as many best practices useful to the Group Policy administrator.

Introduced in Windows® 2000 Server, Group Policy provides directory-based desktop configuration management. 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 Windows Server 2003 family of operating systems, extends Group Policy in a number of ways—through GPMC, which includes scripting interfaces, Group Policy Results, Group Policy Modeling, and more.

The Group Policy settings that you create are contained in a Group Policy object (GPO). By linking a GPO with selected Active Directory® service system containers—sites, domains, and organizational units—you can apply these settings to the users and computers in those Active Directory containers. To create GPOs, you use GPMC in conjunction with the Group Policy Object Editor, an MMC snap-in, also known previously as the Group Policy snap-in, Group Policy Object Editor, or GPedit.

Administrative Requirements for Using Group Policy

In order to use of all of its features, Group Policy requires Active Directory and client computers running Windows 2000 or later. To set Group Policy for a selected Active Directory container, you must have a Windows 2000 or Windows Server 2003 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 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, see the Active Directory white papers at http://www.microsoft.com/ad. Information on planning and implementing Active Directory is available from the Windows Deployment and Resource Kits page at http://www.microsoft.com/reskit.

GPMC System Requirements

GPMC can manage both Windows 2000 and Windows Server 2003 domains with Active Directory. In either case, the computer on which the tool itself runs must be running Windows Server 2003 or Windows XP Professional (with Windows XP Service Pack 1 and the Microsoft .NET Framework). Note: When installing GPMC on Windows XP Professional with SP1, a post SP1 hotfix is required. This hotfix (Q326469) is included with GPMC. GPMC Setup prompts you to install Windows XP QFE Q326469 if it is not already present.

Feedback on this Paper

If you have any comments about this paper, contact mailto:gpdocs@microsoft.com.

What's New About Group Policy in Windows Server 2003

This section summarizes new features in Windows Server 2003 Group Policy. The biggest change for Group Policy in Windows Server 2003 is the introduction of GPMC, the new solution for Group Policy management that helps you manage an enterprise more cost-effectively. It consists of a new Microsoft Management Console (MMC) snap-in and a set of scriptable interfaces for managing Group Policy. GPMC is available for download from the Microsoft GPMC Web site at http://www.microsoft.com/windowsserver2003/gpmc. This paper assumes you are using GPMC.

Group Policy Management Console

GPMC simplifies the management of Group Policy by providing a single place for managing core aspects of Group Policy. It addresses the top Group Policy deployment requirements by providing the following functionality:

- A user interface that makes Group Policy much easier to use.
- Backup/restore of GPOs.
- Import/export and copy/paste of GPOs and Windows Management Instrumentation (WMI) filters.
- Simplified management of Group Policy–related security.
- HTML reporting for GPO settings and Resultant Set of Policy (RSoP) data.
- Scripting of policy-related tasks that are exposed within this tool (not scripting of settings within a GPO).

GPMC is used to create, view, and manage GPOs while the Group Policy Object Editor is used to edit GPOs.

More information about GPMC is contained throughout this paper. For additional information about GPMC including step-by-step instructions for completing tasks, see the following resources:

- Group Policy Administration using the Group Policy Management Console. This white paper provides additional technical details of functionality in GPMC.
- GPMC Help. Available when you install GPMC, this provides step-by-instructions for GPMC tasks and addresses key concepts in GPMC.
- Microsoft GPMC Web site at http://www.microsoft.com/windowsserver2003/gpmc/. This site provides links to the latest GPMC resources including downloading information.

New policy settings

Windows Server 2003 includes more than 200 new policy settings. The new Windows Server 2003 policy settings allow administrators to control the behavior of:

- System restore, error reporting, PC Health.
- Terminal server.
- Networking such as SNMP, Quality of Service (QoS), personal firewall, and dialup connections.
- DNS and net logon.
- Roaming user profiles and Group Policy.
- Control panel.

- Windows Media® Player.
- Wireless configuration.
- Software restriction policy.

Administrative Templates Changes

For Administrative Templates policy settings, Group Policy Object Editor provides explain text directly in the Web view of the console. You also can find this explain text by double-clicking the policy setting and then clicking the **Explain text** tab. In either case, this text shows operating system requirements, defines the policy setting, and includes any specific details about the effect of enabling or disabling the policy setting.

Because new Administrative Template policy settings have been added that only work on specific versions of the operating system such as Windows XP Professional or Windows Server 2003, you can view only the Administrative Template policy settings that might be applied in your users' work environment, based on the “supported” keyword in each Administrative Template (.adm) file. For example, you may want to edit only policy settings that could be applied on client computers running Windows 2000 Service Pack 3. In Group Policy Object Editor, you can specify these options in the **Filtering** dialog box, available by clicking a node in the Administrative Templates section, clicking the **View** menu, and then clicking **Filtering**. For more information, see the section Using Administrative Templates in this paper.

Command Line Refresh of Policy

Administrators can now refresh policy settings from the command line using Gpupdate, which replaces **secedit /refreshpolicy** in Windows 2000. Gpupdate gives administrators better control and flexibility in refreshing policy. For more information, see the section Refreshing Policy from the Command Line in this paper.

WMI Filtering

WMI makes a large amount of data, such as hardware and software inventory, settings, and configuration information, available for a target computer. WMI retrieves data from the registry, drivers, file system, Active Directory, SNMP, MSI, SQL, networking, and Exchange. WMI Filtering in Windows Server 2003 allows you to create queries based on this data. These queries (also called WMI filters) determine which users and computers receive all of the policy configured in the GPO where you create the filter. This functionality lets you target Group Policy based on a significant number of different properties of the target. In most organizations only senior administrators would actually create WMI filters; other administrators would simply access the WMI filters that have been created for their domain. For more information, see the section WMI Filtering in this paper.

Tools for Best Practice Organizational Unit Design

Redirusr.exe (for user accounts) and Redircomp.exe (for computer accounts) are two new tools included with Windows Server 2003 that enable you to change the default location where new user and computer accounts are created so you can more easily scope GPOs directly to newly created user and computer objects. By running Redirusr.exe and Redircomp.exe once for each domain, the domain administrator can specify the organizational units into which all new user and computer accounts are

placed at the time of creation. For more information, see the section Redirecting the Users and Computers Containers in Windows Server 2003 Domains in this paper.

Forest Trust

The Windows Server 2003 family introduces a new feature called Forest Trust that enables you to authenticate and authorize access to resources from separate, networked forests. With trusts established between forests, you can manage Group Policy throughout your enterprise, which provides greater flexibility especially in large organizations. For more information, see the section Using Group Policy Features Across Forests in this paper.

Domain Rename

The ability to rename a domain provides you with the flexibility to make important changes to your forest structure and namespace as the needs of your organization change. Renaming domains can accommodate acquisitions, mergers, name changes, or reorganizations. Domain rename allows you to:

1. Change the DNS and NetBIOS names of any domain in the forest (including the forest root domain).

2. Restructure the position of any domain in the forest (except the forest root domain).

You can only rename domains in a forest where all of the domain controllers are running Windows Server 2003 and the forest functional level has been raised to Windows Server 2003. For more information, see Windows Server 2003 Domain Rename Tools at http://www.microsoft.com/windowsserver2003/downloads/domainrename.mspx.

Restore GPOs tool

This is a new command-line tool intended for failure recovery. The tool, dcgpofix.exe, restores the default GPOs to their original state (that is, the default state after initial installation). For more information, see “Troubleshooting Windows Server 2003 Group Policy” available from the Microsoft GPMC Web site at http://www.microsoft.com/windowsserver2003/gpmc/.

Wireless Support

A new Wireless Network (IEEE 802.11) Policies Group Policy extension allows you to configure wireless network settings that are part of Group Policy for Computer Configuration. Wireless network settings include the list of preferred networks, Wired Equivalent Privacy (WEP) settings, and IEEE 802.1X settings. These settings are downloaded to targeted domain members, making it much easier to deploy a specific configuration for secure wireless connections to wireless client computers.

Software Restriction Policy Settings

Software restriction policy settings address the need to regulate unknown or untrusted software. With the rise in the use of networks, the Internet, and email for business computing, users find themselves exposed to new software in a variety of ways. Users must constantly make decisions about running unknown software. Viruses and Trojan horses often intentionally misrepresent themselves to trick users into running them. It is difficult for users to make safe choices about which software they should run.

With software restriction policy settings, you can protect your computing environment from untrusted software by identifying and specifying which software is allowed to run. You can define a default security level of unrestricted or disallowed for a GPO so that software is either allowed or not allowed to run by default. You can make exceptions to this default security level by creating rules for specific

software. For example, if your default security level is set to disallowed, you can create rules that allow specific software to run. For more information, see the section Software Restriction Policy Settings in this paper.

Internet Explorer Enhanced Security Configuration

Internet Explorer Enhanced Security Configuration, also known as Internet Explorer hardening, is enabled by default on computers running Windows Server 2003. It can be managed using Group Policy in an enterprise environment to ensure consistent trusted sites and security settings on targeted server computers or to disable the feature on specific servers. For example, you may wish to ensure that Internet Explorer Enhanced Security Configuration is reapplied on a specific computer if the local administrator on that computer turns it off using the Optional Component Manager in the Windows Components Wizard (available from Add or Remove Programs.) In addition, it's likely that you will want to manage computers or groups of computers in your organization by defining a set of trusted sites and/or a specific security level for sites in the Internet or Trusted sites zones. For more information, see Using Group Policy and Internet Explorer Enhanced Security Configuration later in this document and Managing Internet Explorer Enhanced Security Configuration, available from the Microsoft Group Policy Web site at http://www.microsoft.com/grouppolicy.

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 GPOs. GPOs are linked to the following Active Directory containers: sites, domains, or organizational units. The settings within the GPOs are then evaluated by the affected clients, using the hierarchical nature of Active Directory.

Linking Group Policy Objects to Active Directory Containers

GPOs cannot be linked directly to users, computers, or security groups. They can only be linked to sites, domains and organizational units.

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

By linking GPOs to sites, domains, and organizational units, 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 organizational units. Note that policy is not inherited across domains.
- A GPO applied to an organizational unit applies directly to all users and computers in the organizational unit and by inheritance to all users and computers in child organizational units.

To link a GPO to a site, domain, or organizational unit, use GPMC. In the console tree, locate the site, domain or organizational unit and then choose **Link an Existing GPO** or **Create and Link a GPO Here**.

Note that GPOs are stored in domains not in organizational units. For example, if you create and link a new GPO for an organizational unit, GPMC is actually completing two steps at once: creating a GPO in the domain and then linking that GPO to that organizational unit. The link is not a component of the GPO; it is a component of the container to which it is linked. Therefore, if you want to delegate the ability to manage links for a given container, it must be delegated on that container, not the GPO. In the GPMC tree view, GPO links on a given container are shown as child nodes of that container.

Although you can link a site, domain, or organizational unit to a GPO in another trusted domain, this is not generally recommended for performance reasons because of the potential delay of processing GPOs at logon.

Group Policy Hierarchy

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

1. **Local GPO.** Each computer has exactly one GPO that is stored locally, shared by all users of that computer. This processes for both computer and user Group Policy processing.
2. **Site.** Any GPOs that have been linked to the site that the computer belongs to are processed next. Processing is in the order that is specified by the administrator, on the **Linked Group Policy Objects**

tab for the site in GPMC. The GPO with the lowest **link order** is processed last, and therefore has the highest precedence.

3. **Domain.** Processing of multiple domain-linked GPOs is in the order specified by the administrator, on the **Linked Group Policy Objects** tab for the domain in GPMC. The GPO with the lowest **link order** is processed last, and therefore has the highest precedence.
4. **Organizational units.** GPOs that are linked to the organizational unit that is highest in the Active Directory hierarchy are processed first, then GPOs that are linked to its child organizational unit, and so on. Finally, the GPOs that are linked to the organizational unit that contains the user or computer are processed.

At the level of each organizational unit in the Active Directory hierarchy, one, many, or no GPOs can be linked. If several GPOs are linked to an organizational unit, their processing is in the order in which GPOs are linked to the organizational unit. For example, if you link three GPOs to an organizational unit the first GPO you added has the highest precedence and overwrites the settings of all other GPOs. Alternatively, you can specify the order on the **Linked Group Policy Objects** tab for the organizational unit in GPMC.

This order means that the local GPO is processed first, and GPOs that are linked to the organizational unit of which the computer or user is a direct member are processed last, which overwrites settings in the earlier GPOs if there are conflicts. (If there are no conflicts, then the earlier and later settings are merely aggregated.)

In GPMC, you can view the precedence order of inherited GPOs for a given site, domain or organizational unit by navigating to the Group Policy Inheritance tab for any site, domain, or organizational unit.

Managing Inheritance of Group Policy

You can further control precedence and how GPO links are applied to specific domains, sites, or organizational units by:

- Changing the link order. Within each domain, site, and organizational unit, the link order controls when links are applied. To change the precedence of a link, you can change the link order, moving each link up or down in the list to the appropriate location. The link with the higher order (with 1 being the highest order) has the higher precedence for a given site, domain, or organizational unit. For example, if you add six GPO links and later decide that you want the last one that you added to have highest precedence, you can move the GPO link to the top of the list. However, the link order of an inherited GPO cannot be altered.
- Blocking Group Policy inheritance. You can block policy inheritance for a domain or organizational unit. Using block inheritance prevents GPOs linked to higher sites, domains, or organizational units from being automatically inherited by the child-level. By default, children inherit all GPOs from the parent, but it is sometimes useful to block inheritance. For example, if you want to apply a single set of policies to an entire domain except for one organizational unit, you can link the required GPOs at the domain level (from which all organizational units inherit policies by default), and then block inheritance only on the organizational unit to which the policies should not be applied. Blocking does not affect Local GPOs.
- Enforcing a GPO link. You can specify that the settings in a GPO link should take precedence over the settings of any child object by setting that link to Enforced (formerly known as “no override”). GPO-links

that are enforced cannot be blocked from the parent container. Without enforcement from above, the settings of the GPO links at the higher level (parent) are overwritten by settings in GPOs linked to child organizational units, if the GPOs contain conflicting settings. With enforcement, the parent GPO link always has precedence. Note that *Enforce* policy options always take precedence over Block Inheritance.

- Disabling a GPO link. By default, processing is enabled for all GPO links. You can completely block the application of a GPO for a given site, domain, or organizational unit by disabling the GPO link for that domain, site, or organizational unit. Note that this does not disable the GPO itself, and if the GPO is linked to other sites, domains or organizational units, they will continue to process the GPO, if their links are enabled.
- Disabling user and/or computer settings. A GPO may have its user settings disabled, its computer settings disabled, or all settings disabled. By default, neither user settings nor computer settings are disabled on a GPO.

Note A GPO link may be enforced, or disabled, or both. By default, a GPO link is neither enforced nor disabled. If the link is enforced and disabled, the disabled link has precedence.

Figure 1 below shows a sample domain structure to illustrate how GPOs can be applied to containers in Active Directory.

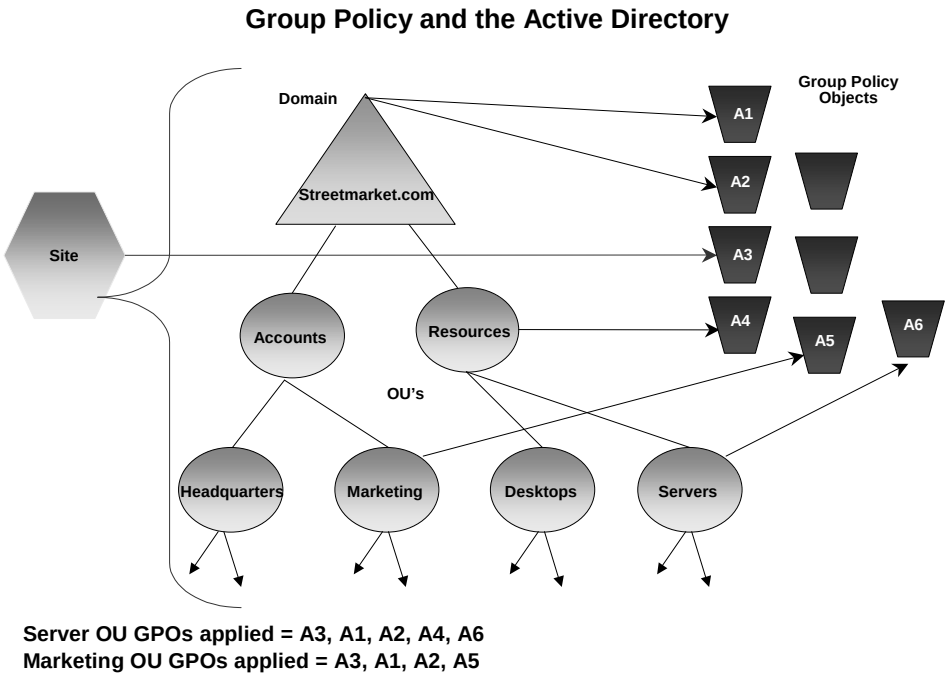


Figure 1. Group Policy and Active Directory

Filtering the Scope of the Group Policy Object

You can further refine which groups of computers and users a particular GPO influences by using security groups or WMI filtering.

Security Filtering

Security filtering is a way of refining which users and computers will receive and apply the settings in a GPO. Using security filtering, you can narrow the scope of a GPO so that it applies only to a single group, user, or computer by specifying that only certain security principals within a container where the GPO is linked apply the GPO. Security filtering determines whether the GPO as a whole applies to groups, users, or computers; it cannot be used selectively on different settings within a GPO.

In order for the GPO to apply to a given user or computer, that user or computer must have both **Read** and **Apply Group Policy (AGP)** permissions on the GPO, either explicitly, or effectively though group membership.

By default, all GPOs have **Read** and **AGP** both **Allowed** for the Authenticated Users group. The Authenticated Users group includes both users and computers. This is how all authenticated users receive the settings of a new GPO when it is applied to an organizational unit, domain or site. Therefore, the default behavior is for every GPO to apply to every Authenticated User. By default, Domain Admins, Enterprise Admins, 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.

You can change these permissions to limit the scope to a specific set of users, groups, or computers within the organizational unit, domain, or site. Group Policy Management manages these permissions as a single unit, and displays the security filtering for the GPO on the GPO Scope tab. Using GPMC, you can add and remove groups, users, and computers to be used as security filters for each GPO. In addition, security principals used for security filtering also appear on the **Delegation** tab for a GPO as having **Read (from Security Filtering)**, since they have read access to the GPO.

To modify security filtering, you add or remove groups in the Security Filtering section on the Scope tab of a GPO. In practice, you don't have to set the two access control entries (ACEs), because GPMC sets both for you when you set security filtering. In addition, The **Read** and **AGP** permissions are visible separately, and able to be set independently of one another, through the access control list (ACL) editor. In GPMC, the **Security Filtering** section of the **Scope** tab of a GPO shows only whether the GPO will apply. If you want to see the permissions separately, you can open the ACL editor by clicking the **Advanced** button on the **Delegation** tab for the GPO.

To prevent a GPO from applying to a specified group requires removal of the **AGP ACE from that group. In the ACL editor, if you remove the AGP ACE** (clear the **Allow check box**) for Authenticated Users, you can then explicitly grant this permission to individual security groups that should receive the policy settings. Alternatively, you could set AGP 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 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, such as a GPO for a human resources group. It might be advisable to limit Read access on GPOs that affect the HR users to only those users.

Security groups and DACLs are also used to delegate control of GPOs, as explained in the section Delegating Group Policy.

Notes

Granting Read and AGP is not sufficient to ensure that the GPO is processed for a user or computer. The GPO also has to be linked to a site, domain or organizational unit containing the user or computer, directly or through inheritance.

A GPO with security filtering set to Read and AGP doesn't necessarily apply to all security principals that have security filtering. It only applies to them if those user or computer objects are in the container or child container that is linked to the GPO.

The location of a security group in Active Directory is irrelevant to security filtering and, more generally, irrelevant to Group Policy processing.

WMI Filtering

WMI filters allow you to dynamically determine the scope of GPOs based on attributes of the target computer.

When a GPO that is linked to a WMI filter is applied on the target computer, the filter is evaluated on the target computer. If the WMI filter evaluates to false, the GPO is not applied (except if the client computer is running Windows 2000, in which case the filter is ignored and the GPO is always applied). If the WMI filter evaluates to true, the GPO is applied.

WMI makes data about a target computer available for administrative use. Such data can include hardware and software inventory, settings, and configuration information. For example, WMI exposes hardware configuration data such as CPU, memory, disk space, and manufacturer, as well as software configuration data from the registry, drivers, file system, Active Directory, the Windows Installer service, networking configuration, and application data.

A WMI filter consists of one or more queries based on this data. If all queries are true, the GPO linked to the filter will be applied. The queries are written using the WMI Query Language (WQL), a SQL-like language. Queries can be combined with AND and OR logical operators to achieve whatever effect the administrator wants. Each query is executed against a particular WMI namespace. When you create a query, you must specify the namespace. The default is root\CIMv2, which is appropriate for most WMI queries. For more information, see Windows Management Instrumentation in the Microsoft Platform SDK at http://msdn.microsoft.com/library/default.asp?url=/library/en-us/wmisdk/wmi/wmi_start_page.asp.

The WMI filter is a separate object from the GPO in the directory. To apply a WMI filter to a GPO, you link the filter to the GPO. This is shown in the WMI filtering section on the Scope tab of a GPO. Each GPO can have only one WMI filter, however the same WMI filter can be linked to multiple GPOs.

WMI filters, like GPOs, are stored on a per-domain basis. A WMI filter and the GPO it is linked to must be in the same domain.

Notes

Client support for WMI filters exists only on Windows XP, Windows Server 2003, and later operating systems. Windows 2000 clients will ignore any WMI filter and the GPO is always applied, regardless of the WMI filter.

WMI filters are only available in domains that have at least one Windows Server 2003 domain controller. In an environment consisting only of Windows 2000 domains, the WMI filter node in GPMC is not shown.

Here are some sample uses of WMI Filters.

- Services – computers where DHCP is turned on.
- Registry – computers that have this registry key populated.
- Hardware inventory – computers with a Pentium III processor.
- Software inventory – computers with Visual Studio® .NET installed.
- Hardware configuration – computers with NICs on interrupt level 3.
- Software configuration – computers with multi-casting turned on.
- Associations – computers that have any service dependent on SNA service.
- Ping – computers that can ping Server1 in less than 100 milliseconds.

WMI filtering allows administrators to filter the application of a GPO by attaching one set of Windows Query Language query to a GPO. The queries can be written to query WMI for multiple items. If the query returns true for all queried items, then the GPO will be applied to the target user or computer. The WMI filter applies to every setting in the GPO, so you will want to create separate GPOs specifically for WMI filtering.

There are two distinct parts to WMI filtering in Windows Server 2003:

- Server administration of WMI filters. This includes GPMC, changes to the Group Policy Object Editor, and filter specifications.
- Client side processing. (WMI supports batch processing of WMI filters.)
- For more information about WMI filtering including sample filters for specific scenarios, see Appendix C in this paper.

MMC Snap-in Extension Model

The nodes of the Group Policy Object Editor are also 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 Object Editor to provide additional policy settings.

For more information on creating MMC extensions, see the Microsoft Management Console section of the Microsoft Platform SDK documentation at: http://www.microsoft.com/msdownload/platformsdk/sdkupdate/.

By default, all the available Group Policy Object Editor extensions are loaded when you start the Group Policy Object Editor. You can modify this default behavior by creating a custom MMC console, or by using policy settings to control the behavior of MMC itself. MMC **options are accessed under the** User Configuration\Administrative Templates\Windows Components\Microsoft Management Console node. For more information, see:

Specifying Group Policy to Control the Behavior of MMC and Snap-ins, later in this document.

Group Policy Object Editor Namespace

The root node of the Group Policy Object Editor 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.Contoso.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 nodes 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 Object Editor

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 .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 and Windows Server 2003 operating systems and their components as well as any registry-based policy settings provided by applications. You use these policy settings 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 .adm files to specify the registry settings that can be modified through the Group Policy Object Editor 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 GPO. You can define local computer, domain, IP security settings, wireless configuration, and software restriction policy settings. For more information on security settings, see Security Settings and Appendix A: Security Settings and User Rights, later in this paper.

- 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 more information on software installation, see Software Installation, later in this document.
- 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 Script 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 Microsoft Windows Script Web site at http://www.microsoft.com/scripting 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.
- Internet Explorer Maintenance. Internet Explorer Maintenance is used to manage and customize Internet Explorer on computers running Windows 2000 or later. You can also export settings for Windows 95, Windows 98, and Windows NT® 4.0-based client computers (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, Favorites, and other options. See Internet Explorer Maintenance, later in this document.
- Folder Redirection. You can use folder redirection to redirect special directories on Windows 2000 or Windows Server 2003 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.

For more information about extending the functionality of the Group Policy Object Editor see "Implementing Registry-Based Group Policy" at http://www.microsoft.com/windows2000/techinfo/howitworks/management/rbppaper.asp.

Client-side Extensions to Group Policy

Some of the Group Policy Object Editor extensions also include client-side extensions. These extensions are 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 GPO 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 Group Policy container 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 Group Policy template is a directory structure within the file system that stores Administrative Template-based policy settings, security settings, script files, and information regarding applications that are available for Software Installation. The Group Policy template is located in Sysvol in the \Policies sub-directory for its domain. GPOs are identified by their globally unique identifiers (GUIDs) and stored at the domain level. Replication of a GPO to other domain controllers happens through two different mechanisms. The Group Policy container is replicated by using Active Directory replication, whereas the Group Policy template is replicated using File Replication Service (FRS). The settings from a GPO are only applied when the

Group Policy container and Group Policy template are synchronized. For additional information on storage of Group Policy information, see *Appendix B: Group Policy Storage*, later in this paper.

Migrating GPOs Across Domains

Taking a GPO in a given domain and creating a new GPO that contains the same set of policies in a different domain is a central function of GPMC.

Although the collection of settings in a GPO is logically a single entity, the data for a single GPO is stored in multiple locations and in a variety of formats; some data is contained in Active Directory and other data (of various types) is stored on the Sysvol file share on the domain controllers. This means that copying GPOs is not as simple as taking a directory and copying it from one computer to another.

In addition to the complex way in which GPO data is stored, certain policy data may be valid in one domain but be invalid in the domain that the GPO is being copied to. For example, Security Identifiers (SIDs) stored in security policy settings are often domain specific. In addition, Universal Naming Convention (UNC) paths for folder redirection or software installation policies may not work properly if the data in the GPO is copied without modification to a different domain.

Migration Tables

The solution is to modify these references in the GPO that are domain-specific, during the import or copy operation, so that the settings in the destination GPO are written with the appropriate information for the destination domain. GPMC supports this capability using migration tables.

A migration table is a file that maps references to users, groups, computers, and UNC paths in the source GPO to new values in the destination GPO. A migration table consists of one or more mapping entries. Each mapping entry consists of a type, source reference, and destination reference. If you specify a migration table when performing an import or copy, each reference to the source entry will be replaced with the destination entry when writing the settings into the destination GPO.

The migration table will apply to any references in the settings within a GPO, whether you are performing an import or copy operation. In addition, during a copy operation, if you choose the option to preserve the discretionary access control list (DACL) on the GPO, the migration table will also apply to both the DACL on the GPO and the DACLs on any software installation settings in the GPO.

Migration tables store the mapping information as XML, and have their own file name extension, .migtable. You can create migration tables using the Migration Table Editor (MTE). The MTE is a convenient tool for viewing and editing migration tables without having to work in, or be familiar with, XML. The MTE is associated with the .migtable extension so that when you double click a migration table, it opens in the MTE. The MTE is installed with GPMC. You can also create and edit migration tables using any XML editor or using the GPMC scripting interfaces.

GPMC as the Solution for Migrating GPOs

There are four operations that GPMC provides to allow for archival and recovery of GPOs, and for migrating GPOs from one environment to another:

- Copy. A copy operation allows you to transfer settings from an existing GPO in Active Directory directly into a new GPO. The new GPO created during the copy operation is given a new GUID and is unlinked. You can use a copy operation to transfer settings to a new GPO in the same domain, another domain in the same forest, or a domain in another forest. Because a copy operation uses an existing GPO in Active Directory as its source, trust is required between the source and destination domains. Copy

operations are suited for moving Group Policy between production environments, and for migrating Group Policy that has been tested in a test domain or forest to a production environment, as long as there is trust between the source and destination domains.

- Backup. Backing up a GPO copies the data in the GPO to the file system. The backup function also serves as the export capability for GPOs. A GPO backup can be used to restore the GPO to the backed-up state, or to import the settings in the backup to another GPO.
- Import. The Import operation transfers settings into an existing GPO in Active Directory using a backed-up GPO in the file system location as its source. Import operations can be used to transfer settings from one GPO to another GPO within the same domain, to a GPO in another domain in the same forest, or to a GPO in a domain in a different forest. The import operation always places the backed-up settings into an existing GPO. It erases any pre-existing settings in the destination GPO. Import does not require trust between the source domain and destination domain. Therefore it is useful for transferring settings across forests and domains that don't have trust. Importing settings into a GPO does not affect its DACL, links on sites domains or organizational units to that GPO, or a link to a WMI filter.
- Restore. Restoring a GPO re-creates the GPO from the data in the backup. A restore operation can be used in both of the following cases: the GPO was backed up but has since been deleted, or the GPO is live and you want to roll back to a known previous state.

Each of these operations can be performed through the GPMC user interface, or through the GPMC scripting model.

For more information, see the following resources:

- Group Policy Administration using the Group Policy Management Console White paper. Provides technical details of functionality in GPMC.
- Migrating GPOs Across Domains with GPMC. Explains how to migrate GPOs from one domain to another using GPMC.
- GPMC Help. Available when you install GPMC, this provides step-by-instructions for GPMC tasks and addresses key concepts in GPMC.

Scripting Group Policy Tasks

GPMC provides a comprehensive set of COM interfaces for scripting many Group Policy-related operations. The interfaces are documented in the Group Policy Management Console SDK, which is located at **%programfiles%\gpmc\scripts\gpmc.chm** on any computer where you installed GPMC. (The Group Policy Management Console SDK is only available in English.)

When you install GPMC, a set of sample scripts illustrating the use of these interfaces are installed to the **%programfiles%\gpmc\scripts** directory.

The sample scripts address real-world administrative problems and scenarios. You can perform various tasks such as finding all GPOs in a domain that have duplicate names or generating a list of all GPOs in a domain whose settings are disabled or partially disabled.

Note Scripted control of individual settings inside a GPO is not provided.

Delegating Group Policy

One of the features of 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.

With GPMC, the following tasks can be delegated:

- Create GPOs in a domain.
- Set permissions on a GPO.
- Set policy-related permissions on site, domain or organizational unit.
    - Link GPOs to a given site, domain or organizational unit.
    - Perform Group Policy Modeling analyses on a given domain or organizational unit (but not on a site).
    - Read Group Policy Results data for objects in a given domain or organizational unit (but not on a site).
- Create WMI filters in a domain.
- Set permissions on a WMI filter.

GPMC simplifies delegation by managing the various ACEs required for a task as a single bundle of permissions for the task. If you want to see the ACL in detail, you can click the **Advanced** button on the **Delegation** tab.

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

You can also specify Group Policy to control the behavior of 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 GPO:

Groups or Users	Security permission
Authenticated User	Read with Apply Group Policy ACE
Domain Admins Enterprise Admins 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 Admins, 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 Organizational Unit

The Group Policy tab in the Properties page for a site, domain, or organizational unit allows the administrator to specify which GPOs are linked to this site, domain, or organizational unit. This property page stores the user's choices in two Active Directory properties called gPLink and gPOptions. The gPLink property contains the prioritized list of GPOs and the gPOptions property contains the Block Policy Inheritance setting.

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

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 organizational unit.

Creating GPOs

By default, only Domain Admins, Enterprise Admins, and Group Policy Creator Owners can create new GPOs. Creating GPOs is a user right of the Group Policy Creator Owners (GPCO) group by default but can be delegated to any group or user. There are two methods to grant a group or user this right:

- Add the user or group to membership of the Group Policy Creator Owners group. This was the only method available prior to GPMC.
- Explicitly grant the group or user permission to create GPOs. This method is newly available with GPMC.

You can manage this permission using the **Delegation** tab on the **Group Policy Objects** container for a given domain in GPMC. This tab shows the groups that have permission to create GPOs in the domain, including the GPCO group. From this tab, you can modify the membership of existing groups with this permission, or add new groups.

The ability to grant users permissions to create GPOs without using GPCO was added to facilitate the delegation of GPO creation to users outside the domain. Because the Group Policy Creator Owners group is a domain global group, it cannot contain members from outside the domain. Thus, prior to GPMC, this task could not be delegated to members outside the domain.

It is recommended that for users and groups within the domain, you continue to use the GPCO group to grant them GPO creation rights. If you require that users outside the domain have the ability to create GPOs, then create a new domain local group in the domain ("GPCO - External"), grant that group GPO creation rights in the domain, and then add external domain users to that group.

Adding a user to the membership of GPCO, or granting the user GPO creation permissions directly using the new method available in GPMC, is identical in terms of permissions. Users have the ability to create GPOs in the domain, but do not have permissions on GPOs created by other users. For example, granting a user the ability to create GPOs in the domain does not give the user the ability to edit or delete existing GPOs, or the ability to link the GPO to a site, domain or organizational unit.

Note that when an administrator creates a GPO, the Domain Admins group becomes the Creator Owner of the GPO. The ability to link GPOs to a site, domain or organizational unit is a permission that is specific to that site, domain or organizational unit. When delegating to non-administrators, you should also consider delegating the ability to manage the links for a specific organizational unit. The reason is that by default, non-administrators cannot manage links.

In GPMC, this permission can be managed using the Delegation tab on the site, domain or organizational unit when you click the Link GPOs option in the permission drop-down list box. At the individual permission level in Active Directory, this allows Read and Write access to the gPLink and gPOptions attributes on the site, domain, or organizational unit. By default, only Domain Admins and Enterprise Admins have this permission.

Editing Group Policy Objects

To edit a GPO, the user must have both read and write access to the GPO. (However, read-only support for opening a GPO is provided in GPMC). 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 default, Domain Admins, Enterprise Admins, the operating system, and the GPO Creator Owner can edit GPOs because they have full control of GPOs without the Apply Group Policy attribute.

Delegating an individual GPO

There are five permission options on GPOs in GPMC user interface. Each corresponds to a set of individual NT permissions. The correspondence is summarized in the following table.

Option in GPMC user interface	Corresponding NT permission in ACL Editor
Read	Allow **Read** Access on the GPO
Edit settings	Allow Read, Write, Create Child Objects, and Delete Child Objects.
Edit, delete, and modify secu	Allow **Read**, **Write**, **Create Child Objects**, **Delete Child Objects**, **Delete**, **Modify Permissions**, ar **Modify Owner**. This essentially grants full control on the GPO, except that the **Apply Group Policy** permission is not set.
Read (from Security Filtering	This setting cannot be set directly, but appears on the delegation tab if the user has **Read** and **App Group Policy** permissions to the GPO.
Custom	Any other combination of permissions, including the use of **Deny** will show up as **Custom** in the display. GPMC can only set custom permission sets by clicking the Advanced button and opening the ACL editor.

Permissions on a GPO are managed from the Delegation tab of that GPO.

Specifying Group Policy to Control the Behavior of MMC extensions

Windows Server 2003 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.

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, select a policy setting, and view the description in the Web view or click the explain tab in the Properties dialog box for the policy setting.

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.

Creating Custom Group Policy Object Editor Consoles

You can create custom Group Policy MMC consoles (.msc files), which include only a subset of the Group Policy Object Editor 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 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 constitutes the main nodes in the Group Policy Object Editor namespace; they are all loaded by default when the Group Policy Object Editor 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

Administrative templates, (or .adm files), enable administrators to control registry settings using Group Policy. Windows comes with a predefined set of Administrative template files, which are implemented as text files (with an .adm extension), that define the registry settings that can be configured in a GPO. These .adm files are stored in two locations by default: inside GPOs in the Sysvol folder and in the %windir%\inf directory on the local computer.

As new versions of Windows are released, new policy settings are added. In addition to supporting these new settings, each successive version of Windows supports all registry policy settings that were available in earlier versions of Windows. For example, the Windows Server 2003 family supports all registry policy settings available in Windows 2000 and Windows XP.

Note that .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 Object Editor and GPMC. 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.

It is important to understand that .adm files are not the actual settings that are deployed to client operating systems. The adm file is simply a template file that provides the friendly name for the setting and an explanation. This template file is used to populate the user interface. The settings that are deployed to clients are contained in the registry.pol file inside the GPO. On Windows XP and Windows Server 2003, each registry setting contains a "Supported on" tag that indicates which operating system versions support that policy setting. If a setting is specified and deployed to a client operating system that does not support that setting, the settings are ignored.

Because all successive iterations of .adm files include settings from earlier versions, and because there is no harm if a new setting is applied inadvertently to a computer running an earlier operating system

that does not support that setting, it is recommended to always create and edit GPOs from a computer that has the latest .adm files available. Note that the behavior for handling .adm files in GPMC and the Group Policy Object Editor differs.

Windows Server 2003 includes the following .adm files: System.adm, Inetres.adm, Conf.adm, Wmplayer.adm, and Wuau.adm, which contain all the settings initially displayed in the Administrative Templates node.

.Adm file	Contains	For Use on	Description
System.adm	Settings to configure the Operating System	Windows 2000 or Windows Server 2003	Loaded by default.
Inetres.adm	Settings to configure Internet Explorer	Windows 2000 or Windows Server 2003	Loaded by default.
Conf.adm	Settings to configure NetMeeting v3	Windows 2000 or Windows Server 2003. Note: This tool is not available on Windows XP 64-Bit Edition and the 64-bit versions of the Windows Server 2003 family.	Loaded by default.
Wmplayer.adm	Settings to configure Windows Media Player	Windows XP, Windows Server 2003. Note: This tool is not available on Windows XP 64-Bit Edition and the 64-bit versions of the Windows Server 2003 family.	Loaded by default.
Wuau.adm	Settings to configure Windows Update	Windows 2000 SP3, Windows XP SP1, Windows Server 2003	Loaded by default.

Handling .adm files in Group Policy Object Editor

- Windows Server 2003, Group Policy Object Editor uses .adm files to display available registry-based policy settings in the Administrative Templates section of a GPO. This includes Group Policy for the Windows Server 2003 operating system and its components and for applications.
- By default it attempts to read .adm files from the GPO (from the Sysvol on the domain controller). Alternatively, the .adm file can be read from the local workstation computer. This behavior can be controlled by a policy setting.
- By default, if the version of the .adm file found on the local computer is newer (based on the time stamp of the file) than the version on the Sysvol, the local version is copied to the Sysvol and is then used to display the settings. This behavior can be controlled by a policy setting.
- If the GPO contains registry settings for which there is no corresponding .adm file, these settings cannot be seen in the Group Policy Object Editor. However, the policy settings are still active and will be applied to users or computers targeted by the GPO.
- 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. Computer-specific settings are written to the Local Machine portion of the registry under HKEY_LOCAL_MACHINE.

Handling .adm files in GPMC

- GPMC uses .adm files to display the friendly names of policy settings when generating HTML reports for GPOs, Group Policy Modeling, and Group Policy Results.
- By default, GPMC uses the local .adm file, regardless of time stamp. If the file is not found, then GPMC will look in the GPO's directory on Sysvol.
- The user can specify an alternate path for where to find .adm files. If specified, this takes precedence over the previous locations.
- GPMC never copies the .adm file to the Sysvol.

For more information, see Recommendations for Managing Group Policy Administrative Template (.adm) Files at http://support.microsoft.com/default.aspx?scid=kb;en-us;816662.

Using Administrative Templates

For Administrative Templates policy settings, the Group Policy Object Editor provides explain text directly in the Web view of the console. You also can find this explain text by double-clicking the policy setting and then clicking the Explain text tab. In either case, this text shows operating system requirements, defines the policy setting, and includes any specific details about the effect of enabling or disabling the policy setting.

New policy settings

Windows Server 2003 includes more than 200 new policy settings. The new Windows Server 2003 policy settings allow administrators to control the behavior of:

- System restore, error reporting, PC Health.
- Terminal Server.
- Networking such as SNMP, QoS, personal firewall, and dialup connections.
- DNS and net logon.
- Roaming user profiles and Group Policy.
- Control panel.

To filter settings based on the “supported on” information: Open the Group Policy Object Editor, click View, and then click Filtering. Select the versions you want to show and click **OK**.

Note Showing only policy settings that can be fully managed is the default setting. You can also show policy settings by supported-on information and show only configured policy settings. In Windows Server 2003, the command Only show configured policy settings is now contained in the Filtering dialog box, shown above.

True Policy Settings Compared with Group Policy Preferences

In Windows 2000 and later, all shipping policy settings set registry keys and values in one of the following locations:

- HKLM\Software\Policies (preferred location).

- HKLM\Software\Microsoft\Windows\CurrentVersion\Policies.
- HKCU\Software\Policies (preferred location).
- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies.

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 policy settings 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, Conf.adm, Wmplayer,adm, and Wuau.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 policy settings are displayed in the Group Policy Object Editor. The following .adm files are loaded:

- System.adm: contains operating system settings
- Inetres.adm: contains Internet Explorer restrictions
- Conf.adm: contains NetMeeting settings
- Wmplayer,adm: contains Windows Media Player settings
- Wuau.adm: contains Windows Update 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 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; or they actually set preference settings and mark the registry with these settings; that is, the registry settings persist.

Creating Custom .adm Files

It is possible to create new .adm files. For example when an application adds Group Policy support, a new .adm file may be necessary to describe the location of the appropriate registry keys and the UI exposed by the Group Policy Object Editor. Through the Group Policy Object Editor, the administrator can optionally add in additional .adm files to the GPO which, by default, will then be copied to the domain controller into the GPO directory.

To view custom .adm files in the Group Policy Object Editor:

- Right click any administrative template node, select View and then click Filtering. In the filtering dialog box, clear the check box for Only show policy settings that can be fully managed and click OK.

Viewing Group Policy Preferences

By default only the settings that are contained in the genuine Group Policy trees (the trees that correspond to the reserved Group Policy registry areas) are visible in the console.

To eliminate use of non-policies, you can enable the policy setting, **Enforce Show Policies Only**, available in **User Configuration\Administrative Templates**, under the **System\Group Policy** nodes.

If you enable this setting, the Show Policies Only command is turned on, and administrators cannot turn it off. As a result, Group Policy displays only true settings; preferences do not appear. If you disable this setting or do not configure it, the Show Policies Only command is turned on by default, but administrators can view preferences by turning off the Show Policies Only command.

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

Impact of GPO Replication

By default, when you add a new domain to the console, GPMC uses the PDC emulator in that domain to help ensure that all administrators are using the same domain controller. For managing sites, GPMC uses the PDC emulator in the user's domain by default. You can change the default choice of domain controller using the Change Domain Controller dialog box in GPMC. If you are located at a remote site with a slow connection to the default domain controller, you may want to do this.

It is important for administrators to consider the choice of domain controller in order to avoid replication conflicts particularly because both Active Directory and FRS use multi-master replication. This is especially important to consider because GPO data resides in both Active Directory and on Sysvol, and two independent replication mechanisms must be used to replicate GPO data to the various domain controllers in the domain. 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.

Important

If multiple administrators manage a common GPO, it is recommended that all administrators use the same domain controller when editing a particular GPO, to avoid collisions in FRS.

Because the Group Policy template is replicated to all domain controllers, the size of the .adm files can have an impact on network bandwidth, particularly where domain controllers are separated by slow links.

Security Settings

You can define a security configuration within a GPO. A security configuration consists of settings applied to one or more security areas supported on Windows 2000 Professional, Windows XP Professional or Windows Server 2003. The specified security configuration is then applied to computers as part of the Group Policy application.

The Security Settings extension of the Group Policy Object Editor complements existing system security tools such as the Security tab on the Properties page (of an object, file, directory, 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 domains on Windows 2000 and Windows Server 2003.
- 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. This 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 policy settings regarding sensitive groups, such as Administrators or Payroll. For example, it may be decided that only Joe and Mary should be members of the 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 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 and Windows Server 2003 (such as 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 GPO.

- Wireless Networking. This lets you configure wireless network settings that are part of Group Policy for Computer Configuration. Wireless network settings include the list of preferred networks, WEP settings, and IEEE 802.1X settings. These settings are downloaded to targeted domain members, making it much easier to deploy a specific configuration for secure wireless connections to wireless client computers.
- Software Restriction Policies. This lets you protect your computer environment from untrusted code by identifying and specifying which applications are allowed to run. With software restriction policies, you can:
  - Control the ability of programs to run on your system. For example, if you are concerned about users receiving viruses through e-mail, you can apply a policy setting that does not allow certain file types to run in the e-mail attachment directory of your e-mail program.
  - Permit users to run only specific files on multi-user computers. For example, if you have multiple users on your computers, you can set up software restriction policy settings in such a way that users do not have access to any software but those specific files that are necessary for their work.
  - Decide who can add trusted publishers to your computer.
  - Control whether software restriction policy settings affect all users or just certain users on a computer.
  - Prevent any files from running on your local computer, organizational unit, site, or domain. For example, if your system has a known virus, you can use software restriction policy settings to stop a computer from opening the file that contains the virus.

Note Software restriction policy settings should not be used as a replacement for antivirus software.

- You can configure security settings policies in Computer Configuration\Windows Settings\Security Settings in the Group Policy Object Editor.

Default Security Templates

Windows 2000 and Windows Server 2003 include three default security templates called Basic. These new default security settings are applied to Windows 2000 or Windows Server 2003 systems that have been installed onto an NTFS partition. When Windows 2000 or Windows Server 2003 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 member servers.
- Basicdc.inf for domain controllers.

The Basic security templates specify default Windows 2000 or Windows Server 2003 security settings for all security areas, with the exception of User Rights and Groups. These templates can be applied to Windows 2000 or Windows Server 2003 systems using the Security Configuration and Analysis MMC snap-in or by using the Secedit.exe command-line tool.

Incremental Security Templates

Windows 2000 and Windows Server 2003 include 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 Object Editor.

These security templates were constructed based on the assumption that they would be applied to computers running Windows 2000 or later and that are configured with Windows 2000 or later 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 and Windows Server 2003.

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 and Windows XP Professional), the Compatible configuration opens up the default permissions for the Users group so that legacy applications are more likely to run. For example, Office 97 should run successfully when users are logged on as a User to a computer running Windows 2000, Windows XP, or Windows Server 2003 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, Windows XP, or Windows Server 2003 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, Windows XP, or Windows Server 2003-based computers that operate in native (or pure) Windows 2000 or Windows Server 2003 environments only. 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 or later. Thus, a Windows 2000 highly secure computer cannot communicate with a client running Windows 95, Windows 98, or Windows NT.

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.

Using Software Installation and Maintenance

You can use the software installation and maintenance feature to install software applications at computer startup, user logon, or on demand. You can also use this feature to upgrade deployed applications, remove earlier applications that are no longer required, and deploy service packs and operating system upgrades. They can ensure that a person cannot install any software from local media, such as a CD-ROM or disk.

This feature also provides for the following situations:

- If users inadvertently delete files from an application it will repair itself.
- If users move from one computer to another their software will always be available to them.
- If users do not have an application installed on their computer and they try to open a document associated with that application, the application will automatically be installed and the document will open.

Deploying software through Group Policy requires applications to use the Windows Installer service, which provides much more than just the capability to install applications. It also protects the integrity of the application against inadvertent mishaps with local files. For example, if a user attempted to use a copy of Microsoft Word that was missing some essential files, the Windows Installer service would reinstall the files from the install point, the next time that the application is launched.

In addition, Windows Installer-based applications that are deployed using Group Policy can install with elevated privileges, meaning users don’t have to be administrators on their local machines to install software that you, as a network administrator, want them to have.

Application repair follows the same logic as on-demand installation. Whenever an application authored by Windows Installer is invoked, the Windows Installer service checks to ensure that the appropriate files are available; if required, files or settings are repaired automatically.

You use Group Policy to define software installation options that specify which applications are to be deployed, upgraded, or removed from a computer. You can apply software installation policies to groups of users or to groups of computers, depending on your organization's needs. There are two methods by which you can install applications on users' computers: assigning and publishing.

Assigning Applications

You can assign applications to either a user or a computer using Group Policy. When you assign applications to a computer, the application is automatically installed the next time the computer is started. When you assign applications to a user with Group Policy, the administrator can choose to either have the application installed on-demand when the user selects the application or in-full when the user next logs on:

- On Demand. If the application is installed on demand, the user's computer is set up with a Start menu shortcut, and the appropriate file associations are created in the registry. To the user, it looks and feels as if the application is already present. However, the application is not fully installed until the user needs the application. When the user attempts to open the application or a file associated with that application, Windows Installer checks to make sure that all the files and parameters of the application are present for the application to properly execute. If they are not present, Windows Installer retrieves and installs them from a predetermined distribution point. Once in place, the application opens.

- Full Install. The full-install option is useful for specific groups of users such as frequent travelers who might require all available applications to be fully installed before they travel. With full install, a user's applications are installed at logon.

Assigning applications makes them resilient — they are available no matter what the user does; for example, if the user removes an application, it will automatically be reinstalled on demand.

Publishing Applications

When you publish an application, it appears in Add or Remove Programs in Control Panel. Users can choose to install published applications. Installation can also be configured to occur automatically when a user attempts to open a file that requires a specific published application. You publish applications when the software is not absolutely necessary for users to perform their jobs.

In order to obtain the full benefits of publishing technology, all published applications should be authored to install using the Windows Installer service. Although you can still publish non-Windows Installer service applications using .ZAP files, you won't get the benefits of elevated privileges as explained earlier, and of course, you won't get the benefits of using Windows Installer either.

A .zap file is a text file that provides a pointer to the setup package, which enables the application to be listed in Add or Remove Programs.

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/techinfo/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 Script Host to include both Visual Basic® Scripting Edition (VBScript) and Jscript® development software script types.

Windows 2000 and later include Windows Script Host, a language-independent scripting host for 32-bit Windows platforms. For more information about Windows Script Host, see the Microsoft Windows Script Web site at 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 in Registry.pol Files 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 Script Host 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 Windows XP Professional, Windows 2000, and the Windows 98-based 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.

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 time out period. (By default, scripts will time-out 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 legacy logon 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 file share):

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

For example, you could redirect a user's My Documents directory to \\Server\Share\%username%. By redirecting the My Documents directory, 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. The My Documents folder is part of the Roaming User Profile (RUP), which 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.

Folder Redirection Improvements for Windows XP and Windows Server 2003

This section provides information on the differences between Windows 2000 and Windows Server 2003.

User Interface changes

The Folder Redirection user interface has been simplified for Windows Server 2003. The main goals of these changes were to simplify the use of Folder Redirection by removing the requirement that administrators be familiar with environment variables such as %USERNAME%.

In addition to the simplified UI, several new redirection options have been added:

- **Create a directory for each user under the root path.** Rather than having to enter a UNC path such as \\server\share\%username%\MyDocuments, the administrator can simply type in the path to the file share such as \\server\share, and Folder Redirection will automatically append the username and the directory name when the policy is applied. This removes the need for administrators to be familiar with environment variables, and minimizes the chances of errors and spelling mistakes.
- **Redirect to home directory (My Documents Only).** Windows Server 2003 and Windows XP allow you to redirect a user's My Documents folder to their home directory. This option is intended only for organizations that have a legacy deployment of home directories and want to transition users to the My Documents metaphor while maintaining compatibility with their existing home directory environment. *You should only select this option if you have already deployed home directories in your organization.*
- Folder redirection treats redirection to the home directory as a special case and certain checks are skipped:
    - Redirection to the home directory is only supported on Windows XP and Windows Server 2003 computers. **Redirection to the home directory policy will fail to apply on Windows 2000 computers.**
    - No security check is performed and no setting of access permissions is done. The administrator must set restrictive permissions on the directory to ensure that proper access is granted. The **Grant the user exclusive rights to My Documents** check box on the settings page of the property sheet is disabled**.**
    - No ownership checks are made. Normally folder redirection will fail if a user is not the owner of the directory they are being redirected to. Because redirection to the home directory is intended for use in a legacy environment, this ownership check is skipped.
    - Users must have the home folder property correctly set on their user object. The folder redirection client side extension retrieves the actual path for the user's home directory from the user object at logon time. Users affected by Folder Redirection Policy must have this path correctly set or folder redirection will not apply.
- **Redirect to a specific path.** This option is intended to allow an administrator to redirect folders to an alternate local drive/partition, or to enter unusual configurations not anticipated by the new user interface. Functionally it works in exactly the same way as the Windows 2000 folder redirection user interface.
- **Redirect to the local user profile.** This option is intended to allow an administrator to redirect the selected folder to the default location in the local user profile, for example: %userprofile%\<Folder Name>. This setting can be used to remove redirection for a particular folder, without removing the GPO. Note: Setting the redirection option to "Not Configured" (or "No Administrative policy specified" in the Windows 2000 UI) **does not** redirect the folder to the local profile, this option means that Folder Redirection is not configured – *if a folder was previously redirected it will continue to be redirected to the previous location.* If an administrator wanted to return the folder to the local user profile they can use this redirection setting.

My Pictures no longer shown in the Folder Redirection Node

To simplify the user interface and to help support the best practice that the My Pictures folder should always follow the **My Documents** folder, the My Pictures folder is not shown in the Folder Redirection node for new GPO's. If you have previously redirected the My Pictures folder separately, the My Pictures node will still appear.

Redirected Folders automatically made available offline

By default in Windows XP and Windows Server 2003, any redirected shell folders such as My Documents, Desktop, Start Menu, and Application Data are automatically made available offline. This is in contrast to Windows 2000, which required administrators to configure the "Administratively assigned offline files" policy setting to ensure all files in the redirected folders were always available offline. This setting was difficult to use with advanced folder redirection, and involved extra administrative overhead.

The default behavior can be overridden by enabling the Do not automatically make redirected folders available offline policy. This setting can be found in the Group Policy Object Editor in the User Configuration\Administrative Templates\Network\Offline Files section.

Note that on Windows Server 2003 Offline files are disabled by default.

More information on Folder Redirection will be available in the white paper, "User Data and Settings Management" at http://www.microsoft.com/grouppolicy.

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 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 the Microsoft 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 certification 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 Earlier 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 original Group Policy Object Editor was created in Windows 2000, 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 clients running

Windows 2000 or later, although Windows 2000 and Windows Server 2003 support auto-configuration packages.

Managing Internet Explorer Maintenance Advanced Settings

You can manage advanced settings for Internet Explorer such as setting a size limit for users' Temporary Internet files. In order to do this, you need to first enable **Preference Mode** for Internet Explorer Maintenance. By default, the **Preference Mode** option is hidden. You access this option by right-clicking **Internet Explorer Maintenance** node and selecting **Preference Mode** on the shortcut 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.

For more information, see this Microsoft Knowledge Base article, How to Set Advanced Settings In Internet Explorer by Using Group Policy Objects.

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 Administration Kit (IEAK) at http://www.microsoft.com/windows/ieak/default.asp.These tools provide options for System Policies and restrictions that administrators can use to specify desktop, shell, and security settings, for example.

Remote Installation Services

Remote Installation Services is an optional component that is included in the Windows Server operating system and works with other Windows Server 2003 technologies to implement the Remote Operating System Installation feature. Administrators use Remote Operating System Installation to remotely install a copy of the Windows XP Professional operating system on supported computers. (Computers that are PC98-compliant ship with a PXE Remote Boot ROM .) 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 the GPOs 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.

Group Policy Modeling and Results

Introduction

Group Policy Modeling and Group Policy Results is a feature of Group Policy that makes implementation, troubleshooting, and planning of Group Policy easier. When multiple GPOs apply to a given user or computer, they can contain conflicting policy settings. For most policy settings, the final value of the policy setting is set only by the highest precedence GPO that contains that setting. Group Policy Modeling and Group Policy Results uses the Resultant Set of Policy (RSoP) infrastructure, available on Windows XP and Windows Server 2003, to present the final set of policy that is applied as well as settings that did not apply as a result of policy inheritance.

Specifically, RSoP helps you determine the following:

- The final value of the setting that is applied as a result of all the GPOs.
- The final GPO that set the value of this setting (also known as the winning GPO).

Precedence details that show any other GPOs that attempted to set this setting and the value that each GPO attempted to set for that policy setting.

Group Policy Results

This represents the actual policy data that is applied to a given computer and user. It is obtained by querying the target computer and retrieving the RSoP data that was applied to that computer. The Group Policy Results capability is provided by the client operating system and requires Windows XP, Windows Server 2003 or later. Outside of GPMC, Group Policy Results is referred to as RSoP - logging mode.

Group Policy Modeling

This is a simulation of what would happen under circumstances specified by an administrator. Group Policy Modeling requires that you have at least one domain controller running Windows Server 2003 because this simulation is performed by a service running on a domain controller that is running Windows Server 2003. With Group Policy Modeling, you can either simulate the RSoP data that would be applied for an existing configuration, or you can perform "what-if" analyses by simulating hypothetical changes to your directory environment and then calculating the RSoP for that hypothetical configuration. For example, you can simulate changes to security group membership, or changes to the location of the user or computer object in Active Directory. Outside of GPMC, Group Policy Modeling is referred to as RSoP - planning mode. Note that although Windows 2000 does not provide the RSoP infrastructure, Group Policy Modeling can be used as an effective way to simulate the affect of Group Policy on Windows 2000 computers.

Using GPMC Reports

In GPMC, resultant set of policy data is obtained using Group Policy Modeling or Group Policy Results wizards. GPMC provides an HTML report of the RSoP data. This report shows the final value of the winning settings and the winning GPO that set that value. When you create a Group Policy Modeling or Group Policy Results report, the report is shown in GPMC under the appropriate node. Right-clicking this report and choosing Advanced View opens the RSoP snap-in, which provides additional

information, enabling you to verify precedence for a policy setting. In the RSoP snap-in, the dialog box for a policy setting contains a Precedence tab, which shows all GPOs that attempted to set a particular setting and the value for each GPO.

RSoP Architecture

Figure 2 below shows the high-level architecture of RSoP for Group Policy Results and Group Policy Modeling.

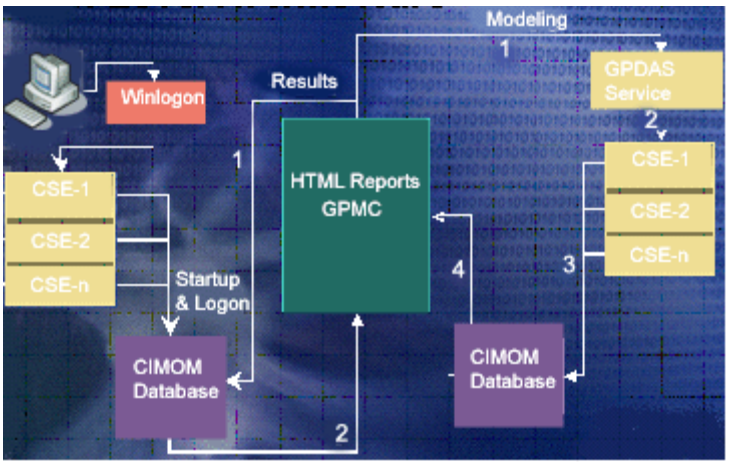


Figure 2. RSoP high-level architecture

Take for example, a standard logon procedure in Windows 2000: a client computer logs onto the network and Winlogon runs. The domain controller passes a list of pointers to the GPOs that are to apply. This list is passed to each of the client-side extensions (CSEs) such as Software Installation, Scripts, Security, Administrative Templates, and so on. Each CSE processes this list of GPOs.

Windows Server 2003 uses the same process but improves on Windows 2000 by collecting all the Group Policy processing information and storing it in a Common Information Model Object Management (CIMOM) database on the local computer. This information, such as the list, content and logging of processing details for each GPO, can then be accessed by tools using WMI.

In Group Policy Results, RSoP queries the CIMOM database on the target computer, receives information about the policies and displays it in GPMC. In Group Policy Modeling, RSoP simulates the application of policy using the Group Policy Directory Access Service (GPDAS) on a Domain Controller. GPDAS simulates the application of GPOs and passes them to virtual client-side extensions on the Domain Controller. The results of this simulation are stored to a local CIMOM database on the domain controller before the information is passed back and displayed in GPMC.

Security and RSoP

By default, access to Group Policy Results is restricted to enterprise, domain, and local administrators although users can still perform logging on their own computer. In Windows XP, non-administrators can run Group Policy Results for their computer and user account; in Windows Server 2003 non-administrators can only run Group Policy Results for their own user account. Group Policy Modeling is restricted to enterprise and Domain Admins. However, organizations can delegate access to Group Policy Results and Modeling using GPMC. For step-by-step instructions, see Group Policy Help.

Group Policy Results and Modeling Examples

Group Policy Results and Modeling allow administrators to solve problems for specific scenarios. Some examples are included below.

Group Policy Results

What is the current state of Folder Redirection for the current user?

Example: User Paul has four computers, and contacts help desk because they cannot find files on computer D that are on computer A, even though Paul is set up to use folder redirection. The administrator runs Group Policy Results and sees that on computer D, redirection is different than the others because a different GPO applies.

What is the current state of Folder Redirection for a sampling of users?

Example: An administrator wants to profile different sets of users. Using Group Policy Results, the administrator picks a sample user from each user group and uses the RSoP information to model redirection within the organization.

Why did this happen?

Example: An administrator is confused as to why Paul's documents are being redirected to the SuperUsers server. The administrator uses Group Policy Results to look at the current redirection path, and the GPO and security group that caused the redirection.

The administrator notices that of the three GPOs specifying folder redirection policy, the winning GPO has the advanced option set to redirect users in different security groups to different locations. The administrator notices that Paul is a member of both the VanillaUsers group and the SuperUsers group and realizes that this caused Paul's folders to be redirected to the SuperUsers server.

Group Policy Modeling

Precedence Details

In processing Group Policy, administrators determine which GPOs were in conflict to configure folder redirection for this user.

Change of Site

Example: An administrator can model site and domain changes for individual users or using a sample target to assess what would happen to an entire group of users under different combinations of sites, domains, and so forth. By comparing what should be seen, by what actually exists under the new GPO structure, the administrator can avoid problems before the move actually takes place.

Example: User Jane is going to move from one department to another. The administrator uses Group Policy Modeling to model the move under the different site condition and finds out that a GPO conflict exists that redirects Jane's folder to an alternate location.

Change of Folder Redirection Mode

An Administrator wants to configure folder redirection to use the advanced options to redirect users to alternate locations based on their security group membership. The administrator uses Group Policy Modeling to configure Group Policy for the desired folder redirection behavior.

By comparing the current results of folder redirection for the users, with the results of the desired changes, the administrator can avoid problems before the move actually takes place.

RSoP Schema

For information about the RSoP schema, see the RSoP SDK, available as part of the Microsoft Windows Platform SDK at http://www.microsoft.com/msdownload/platformsdk/sdkupdate/.

Group Policy Processing

As described earlier in this paper, Group Policy is processed in the following order: Local Group Policy Object (Local GPO), then GPOs linked to containers in this order: site, domain, and organizational units, including any nested organizational units (starting with the organizational unit further from the user or computer object). This means that the local Group Policy Object is processed first, and the organizational unit 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:

- WMI or security filtering that has been applied to GPOs.
- Any domain-based GPO (not local GPO) may be enforced by using the **Enforce** option so that its policies cannot be overwritten. When more than one GPO has been marked as enforced, the GPO that is highest in Active Directory hierarchy takes precedence.
- At any domain or organizational unit, Group Policy inheritance may be selectively designated as Block Inheritance. However, blocking inheritance does not prevent policy from **enforced** 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 a stand-alone computer. The Local GPO can't be blocked by domain-based GPOs. However, settings in domain GPOs always take precedence since they are processed after the Local GPO.

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. (As explained below, Windows XP with Fast Logon enabled lets users logon while Group Policy is processed in the background.)

Synchronous and 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 GPO 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.

Fast Logon in Windows XP Professional

By default in Windows XP Professional, the Fast Logon Optimization feature is set for both domain and workgroup members. This results in the asynchronous application of policies when the computer starts and when the user logs on. This application of policies is similar to a background refresh process and

can reduce the length of time it takes for the Logon dialog box to display and the length of time it takes for the shell to be available to the user. An administrator can change the default by using the Group Policy Object Editor.

Fast Logon Optimization is always off during logon under the following conditions:

- When a user first logs on to a computer.
- When a user has a roaming user profile or a home directory for logon purposes.
- When a user has synchronous logon scripts.

Note that under the preceding conditions, computer startup can still be asynchronous. However, because logon is synchronous under these conditions, logon does not exhibit optimization.

The following table summarizes the default processing of policy on Windows XP.

Client	Application at startup/log on	Application at refresh
Windows 2000	Synchronous	Asynchronous
Windows XP Professional	Asynchronous	Asynchronous

Windows XP clients support Fast Logon Optimization in any domain environment. To turn off Fast Logon Optimization, you can use the following policy setting:

Computer Configuration\Administrative Templates\System\Logon\ Always wait for the network at computer startup and logon

---

Note Fast Logon Optimization is not a feature of Windows Server 2003.

Folder Redirection and Software Installation Policies

Note that when logon optimization is on, a user may need to log on to a computer twice before folder redirection policies and software installation policies are applied. This is because application of these types of policies require the synchronous policy application. During a policy refresh (which is asynchronous), the system sets a flag that indicates that the application of folder redirection or a software installation policy is required. The flag forces synchronous application of the policy at the user's next logon.

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. This is because a policy refresh causes the Windows shell to be refreshed, which in turn causes all open shortcut menus to close, a brief flicker of the screen, and so on. In addition, it causes computers to contact domain controllers more frequently, increasing the load on the domain controllers. However, setting a shorter interval may be useful in test or demonstration scenarios.

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.

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.

Refreshing Policy from the Command Line

Gpupdate refreshes local Group Policy settings and Group Policy settings that are stored in Active Directory, including security settings. This command supersedes the now obsolete **/refreshpolicy** option for the **secedit** command.

Syntax

Gpupdate [/target:{computer | user}] [/force] [/wait:*Value*] [/logoff] [/boot]

Parameters

/target:{computer | user}

Processes only the *Computer* settings or the current *User* settings. By default, both the computer settings and the user settings are processed.

/force

Ignores all processing optimizations and reapplies all settings.

/wait:*Value*

Number of seconds that policy processing waits to finish. The default is 600 seconds. 0 equals no wait, and -1 equals wait indefinitely.

/logoff

Logs off after the refresh has completed. This is required for those Group Policy client-side extensions that do not process on a background refresh cycle but that do process when the user logs on, such as user Group Policy Software Installation and Folder Redirection. This option has no effect if there are no extensions called that require the user to log off.

/boot

Restarts the computer after the refresh has completed. This is required for those Group Policy client-side extensions that do not process on a background refresh cycle but that do process when the computer starts up, such as computer Group Policy Software Installation. This option has no effect if there are no extensions called that require the computer to be restarted.

/synch

Causes the next foreground policy application to be done synchronously. Foreground policy applications occur at computer boot and user logon. You can specify this for the user, computer, or both using the /Target parameter. The /Force and /Wait parameters will be ignored if specified.

/?

Displays help at the command prompt.

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 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 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 a flag to indicate to client-side extensions that a policy setting is being applied across a slow link. Individual client-side extensions can determine whether or not to apply a policy setting 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 switching 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 and Windows Server 2003 use an IP ping algorithm to ping the server, rather than measuring the file system performance method that was used in Windows NT 4.0. Note: Slow link detection requires the Internet Control Message Protocol (ICMP). If ICMP cannot be used to communicate with the domain controllers, policy processing will not work, in which case you should disable slow link detection.

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 KB) * (1000 millisec/sec) / DELTA Average millisec = X
7. X = (4000 KB/sec) / DELTA Average
8. Z Kilobits per second (Kbps) = (4000 KB/sec) / DELTA Average) *(8 bits/byte)
9. Z Kbps = 32000 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 time-out for user profiles policy is located in the Computer Configuration\Administrative Templates\System\Logon node. This policy has support for both pinging 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 check box 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 during logon. For example, if users connecting through a VPN connection are logging in via cached credentials, folder redirection settings will not be processed, because folder redirection policy can only be processed at user logon, not in the background refresh.

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

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 (located in Computer Configuration\Administrative Templates\System\Group Policy). Each policy includes a maximum of three options (check boxes). 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 56 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 credentials) 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\GPExtentions\{82...}\MaxNoGPOListChangesInterval, 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 check box	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)	Users' files could be in use while they are logged on.
Software Installation	Background processing (Do not apply during periodic background processing)	Users' software could be in use while they are logged on.

Policy Settings for Group Policy

You can use administrative templates to configure how you use Group Policy. Policy settings are located in the following areas of the Group Policy Object Editor:

- **Computer Configuration\Administrative Templates\System\Group Policy**
- User Configuration\Administrative Templates\System\Group Policy

For details 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 Replication and Domain Controller Selection

In a domain that contains more than one domain controller, Group Policy information takes time to propagate, or replicate, from one domain controller to another. Low bandwidth network connections between domain controllers slow replication. The Group Policy infrastructure has mechanisms to manage these issues.

Each GPO is stored partly in the Sysvol on the domain controller and partly in Active Directory. GPMC and Group Policy Object Editor present and manage the GPO as a single unit. For example, when you set permissions on a GPO in GPMC, GPMC is actually setting permissions on objects in both Active Directory and the Sysvol. It is not recommended that you manipulate these separate objects independently outside of GPMC and the Group Policy Object Editor. It is important to understand that these two separate components of a GPO rely on different replication mechanisms. The file system portion is replicated through File Replication Service (FRS), independently of the replication handled by Active Directory.

Lack of synchronization between the Group Policy template (data stored on Sysvol) and Group Policy container (data stored in Active Directory) portions of the Group Policy Object can occur temporarily because of the differences in the replication schemes used by Active Directory and FRS.

For those Group Policy extensions that store data in only one data store (either 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 (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 Active Directory and Sysvol is Software Installation. The script files are stored on Sysvol and the Windows Installer package definition is in 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 Policy.

The tools used to manage Active Directory and Group Policy, such as GPMC, the Group Policy Object Editor, and Active Directory Users and Computers all communicate with domain controllers. If there are several domain controllers available, changes made to objects like users, computers, organizational units, and GPOs may take time to appear on other domain controllers. The administrator may see different data depending on the last domain controller on which changes were made and which domain controller they are currently viewing the data from.

For example, if you create a GPO on one domain controller and immediately attempt to link it on another domain controller, the operation could fail. In each domain, GPMC uses the same domain controller for all operations in that domain, in order to avoid any synchronization issues. This includes all operations on GPOs, organizational units, and security groups in that domain. In addition, when the Group Policy Object Editor is opened from GPMC, it will also use the same domain controller in use by GPMC. Finally, GPMC uses the same domain controller for all operations on sites within a given forest. This domain controller for sites is used to read and write information about the links to GPOs that exist

on any given site; information regarding the GPO itself is obtained from the domain controller of the domain hosting the GPO. This domain controller is used to read and write information about the links to GPOs that exist on any given site; information regarding the GPO itself is obtained from the domain controller of the domain hosting the GPO.

By default, when you add a new domain to the console, GPMC uses the PDC emulator in that domain to help ensure that all administrators are using the same domain controller. For managing sites, GPMC uses the PDC emulator in the user's domain by default. You can change the default choice of domain controller using the Change Domain Controller dialog box in GPMC. If you are located at a remote site with a slow connection to the default domain controller, you may want to do this.

It is important for administrators to consider the choice of domain controller in order to avoid replication conflicts particularly because both Active Directory and FRS use multi-master replication. This is especially important to consider because GPO data resides in both Active Directory and on Sysvol, and two independent replication mechanisms must be used to replicate GPO data to the various domain controllers in the domain. 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.

Important

If multiple administrators manage a common GPO, it is recommended that all administrators use the same domain controller when editing a particular GPO, to avoid collisions in FRS.

Options governing selection of a domain controller for GPMC

In GPMC, when you right-click a domain or the sites container and click **Change Domain Controller**, you see a **Change Domain Controller** dialog box. The domain controller options for GPMC are:

- The one with the Operations Master token for the PDC emulator. This is the default and preferred option.
- Use any available domain controller. This is the least safe option.
- Use any available domain controller that is running Windows Server 2003 or later. This option is useful if you are restoring deleted GPOs that contain software installation settings. If possible, it is recommended to perform restoration of GPOs containing software installation settings on domain controllers running Windows Server 2003.
- This domain controller. This option allows you to choose a specific domain controller from a list of domain controllers in the domain.

If you are changing the domain controller for a site, you can also choose any available trusted domain from the Look in this domain drop-down list box in the Change Domain Controller dialog box.

When you open the Group Policy Object Editor from GPMC it always uses the same domain controller that is targeted in GPMC for the domain where that GPO is located.

- 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 Object Editor.

Specifying a Domain Controller by Using Group Policy

Domain Admins 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 option to choose a domain controller is unavailable since a policy is in place that overrides any setting that the user chooses. This policy allows Domain Admins to mandate that all administrators must use the PDC emulator, for example.

The Group Policy domain controller selection policy setting is available in the Administrative Templates node for User Configuration, in the System\Group Policy sub-container.

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 Object Editor focused on the local computer. You can access the Group Policy Object Editor tool by typing mmc at the command prompt, adding the Group Policy Object Editor to MMC console, and focusing the Group Policy Object Editor on the local computer. Group Policy is processed in this order: local GPO first, followed by Active Directory linked GPOs (site, domain, organizational unit, and any nested organizational units).

Local Group Policy Object

On all computers, an Local GPO exists—this is just the Group Policy template portion. The location of the Local GPO 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 Object Editor extensions open when the Group Policy Object Editor is focused on the Local GPO.

Group Policy Object Editor extension	Loaded when Group Policy Object Editor focused on Local GPO
Security Settings	Yes
Administrative Templates	Yes
Software Installation	No
Scripts	Yes
Folder Redirection	No
Internet Explorer Maintenance	Yes

Local Group Policy Object and DACLs

There is no **Apply Group Policy** ACE for the local GPO; therefore, if you have Read access to the Local GPO, the local GPO applies to you. The implication is that it's difficult to have to choose whom the Local GPO should apply to (for example, the Local GPO also applies to the administrator). Everyone with Read access to the Local GPO who logs on gets the Local GPO. 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 Local GPO doesn't apply to that user. This is useful for administrators who don't want to be subject to the Local GPO settings. However, without Read access, administrators cannot see the contents of the Local GPO.

Viewing Policy settings When the Group Policy Object Editor is Focused on the Local Computer

When administrators run the Group Policy Object Editor focused on a local computer, this shows the information in the local GPO, not the cumulative effect of what has been applied to the computer or user. For Windows Server 2003, 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 organizational unit).

Local Group Policy Object Processing

When a computer is joined to a domain with Active Directory and Group Policy implemented, a local Group Policy Object is processed. Note that Local GPO 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, Local GPO policy is applied.

Modifying the Local GPO on a Domain-based Computer

If you modify the Local Group Policy object for a computer that is participating in a domain while the computer is disconnected from the network, the change is applied only after the computer is reconnected to the network. This is caused by two facts: the entire domain hierarchy must first be evaluated to find the resultant set of policy settings that apply to the computer and domain user, and domain-based Group Policy settings always take precedence over local Group Policy settings. Therefore, the computer can use only the existing policy settings (no new policy changes can be evaluated) until the computer is reconnected to the network.

Group Policy Loopback Support

Group Policy is applied to the user or computer, based upon where the user or computer object is located in 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 Admin privileges.

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

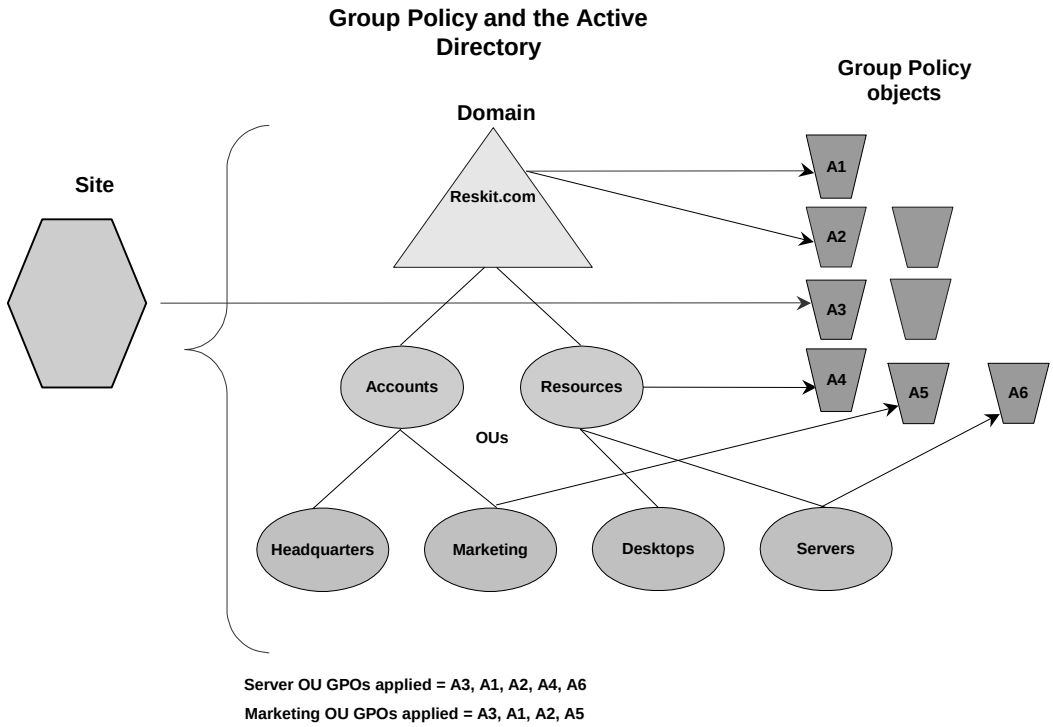


Figure 3. The Reskit domain

Normal user Group Policy processing specifies that computers located in the Servers organizational unit have the GPOs A3, A1, A2, A4, and A6 applied (in that order) during computer startup. Users of the Marketing organizational unit have GPOs A3, A1, A2, and 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 organizational unit to be installed while they are logged on to the computers in the Servers organizational unit. 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 organizational unit:

- **Merge mode**. In this mode, the computer's GPOs have higher precedence than the user's GPOs. In this example, the list of GPOs for the computer is A3, A1, A2, A4, and 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 engine, which is the part of Group Policy that runs in the Winlogon process. 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.

Using Loopback for Terminal Services

You can apply GPOs to Terminal Servers exclusively with the use of a GPO Loopback policy. This policy directs the system to apply the set of GPOs for the computer to any user who logs on to the computer affected by this policy. This policy is intended for special-use computers, such as those in public places, laboratories, and classrooms, where you must modify the user policy based on the computer that is being used. Without Loopback, the user's GPOs determine which user policies apply. If this policy is enabled, the location of a user's computer object is the main factor in determining which set of GPOs are to be applied.

Loopback Processing and Security Filtering

In security filtering, if you have used the Deny ACL to explicitly prevent a policy setting from applying to a computer, the setting could still apply in loopback replace mode because the user's security principal remains unaffected by the Deny ACL computer settings.

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 organizational unit structure, and highlights recommendations for the use of GPOs.

Organizational Unit Structure

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

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

In general, do not try to model your organizational unit structure based on your business organization. Rather, design your organizational unit structure based on how you administer your business. Information on planning for Active Directory is available in Best Practice Active Directory Design for Managing Windows Networks at http://www.microsoft.com/technet/prodtechnol/ad/windows2000/plan/bpaddsgn.asp.

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

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

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

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

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

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

- Deep organizational unit model: link to GPOs at site, domain, and organizational unit with security groups filtering and DACLs or WMI filtering. As a secondary method, use Block Policy Inheritance and Enforce Policy options.

Design Principles

This section presents general guidelines for using GPOs 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 organizational unit 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 policy settings in GPOs. Network administrators can define groups of administrators (for example, Software Installation administrators), and then provide them read and write access to selected GPOs, allowing the network administrator to delegate control of the GPO 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 described earlier in the Delegating Group Policy section.

Separate Users and Computers into Different organizational units

It's recommended that you separate users and computers into separate organizational units. 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.

- For increased security and ease of administration, you should specify different organizational units for all new user and computer accounts when they are created, as explained below.

Redirecting the Users and Computers Containers in Windows Server 2003 Domains

New user and computer accounts are created in the CN=Users and CN=Computers containers by default. It is not possible to apply Group Policy directly to these containers, although they inherit GPOs linked to the domain.

Redirusr.exe (for user accounts) and Redircomp.exe (for computer accounts) are two new tools included with Windows Server 2003 that enable you to change the default location where new user and computer accounts are created so you can more easily scope GPOs directly to newly created user and computer objects. These tools are located in %windir%\system32. By running Redirusr.exe and Redircomp.exe once for each domain, the domain administrator can specify the organizational units into which all new user and computer accounts are placed at the time of creation. This allows administrators to manage these unassigned accounts by using Group Policy before the administrators assign them to the organizational unit in which they are finally placed. You might want to consider restricting the organizational units used for new user and computer accounts by using Group Policy to increase security around these accounts.

For more information about redirecting users and computers, see article 324949, “Redirecting the Users and Computers Containers in Windows Server 2003 Domains,” in the Microsoft Knowledge Base. To find this article, see the Microsoft Knowledge Base link on the Web Resources page at http://www.microsoft.com/windows/reskits/webresources.

For more information about the redirusr.exe and redircomp.exe tools, see the Redirecting Users and Computers link on the Web Resources page at http://www.microsoft.com/windows/reskits/webresources.

Best Practice Organizational Unit Structure

Because you cannot apply Group Policy directly to the CN=Users and CN=Computers containers, if you wanted to define policy settings for users and computers to be stored in their default container you needed to do so on the root of the domain. To prevent policy settings that are defined on a superior container (the root of the domain) from applying to users, computers, and groups in subordinate CN and organizational unit containers, you needed to define complex ACLs on the policy setting in the root of the domain.
The solution for Windows 2000 and Windows Server 2003 domains is to deploy the best-practice organizational unit structure where Users, Computers, Groups, Service Accounts and Admin accounts are each in their own organizational unit.

The following list describes the benefits of using the best-practice organizational unit structure:

- It permits administrators to link GPOs directly to the containers that are hosting users and computers.
- It permits administrators to match GPOs to objects of a common object class. For example, User or Computer policy settings can be linked directly to organizational units that are hosting user or computer accounts.
- It permits non-administrators to apply policy on containers that are not hosting security-sensitive users and groups such as Domain Admins, Schema Admins, or Enterprise Admins.

- It can minimize the effect if an organizational unit is accidentally deleted (this assumes that the parent container is correctly protected).
- It permits you to restore users and groups independently of each other in recovery scenarios. User accounts must exist before the restoration of the group. Having users and groups reside in different containers permits you to restore them and mark them as authoritative independently of each other.

Note that the CN=USERS and CN=COMPUTERS containers are computer-protected objects. You cannot (and must not) remove them for backward compatibility purposes although they can be renamed.

The best-practice organizational unit structure works well for storing existing users, computers, and groups in Active Directory because those objects can be moved into the appropriate organizational unit container on Windows 2000 and Windows Server 2003 domains regardless of its domain or forest functional level. New user accounts, computer accounts, and security groups that are created with earlier-version APIs used by GUI and command-line management tools do not allow administrators to specify a target organizational unit. As a result, these objects will initially be created in the CN=Users and CN=Computers containers until they are moved by the administrator or an administrator-defined script.

For more information about best-practice organizational unit structure see the "Creating an Organizational Unit Design" section of the Best Practice Active Directory Design for Managing Windows Networks at http://www.microsoft.com/technet/prodtechnol/ad/windows2000/plan/bpaddsgn.asp

Functional Compared with Geographical Organizational Unit Structure

When organizing organizational units, 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 organizational unit 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 GPOs 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 GPOs, the longer logon will take to process them. During logon time, each GPO from the user's site, domain, and organizational unit 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 Enforce Feature

You can also ensure that the policy settings you specify in a given GPO at a higher-level parent Active Directory container are enforced on lower-level parent Active Directory containers by using the Enforce 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 policy settings with computer-specific policy settings. This is useful when you want to provide a specific desktop configuration regardless of which users log on to the computer, such as a kiosk or other public terminal. To set User Configuration per computer, you would use the Administrative Templates node under Computer Configuration in the Group Policy Object Editor. For more information on this feature, see Group Policy Loopback Support.

Avoid Using Cross-Domain GPO Assignments

Although you can assign GPOs 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.

Avoid Editing the Default Domain GPO

Instead of editing the default domain GPO, create a new GPO, link it to the domain GPO, and set the new GPO to have precedence over the default domain GPO.

Design Examples

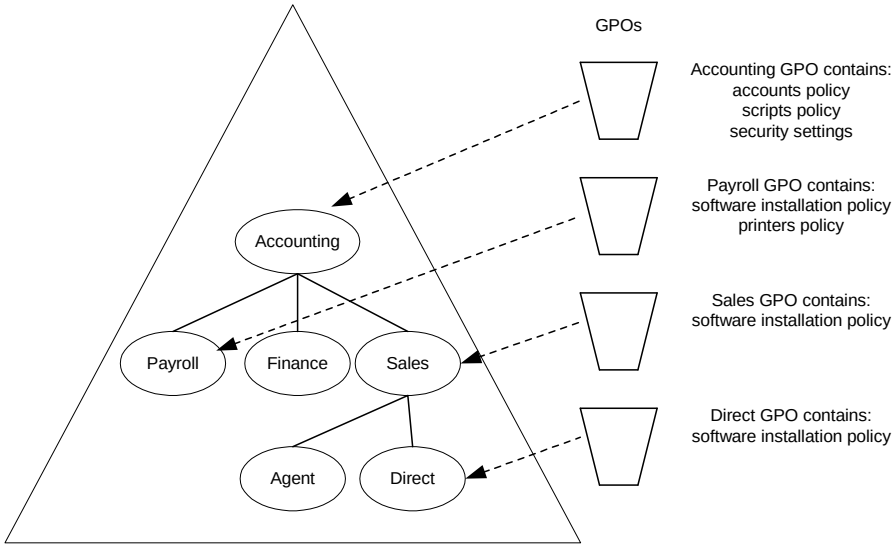
This section presents several models of GPO design. These examples are not intended as guidelines, but they do illustrate various ways to approach GPO design. In most corporate environments, administrators may use a combination of these or similar models, tailored to their business requirements.

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 GPOs based on a layered approach. This approach optimizes maintenance of GPOs and facilitates delegation.

The following graphic illustrates an example of this model.

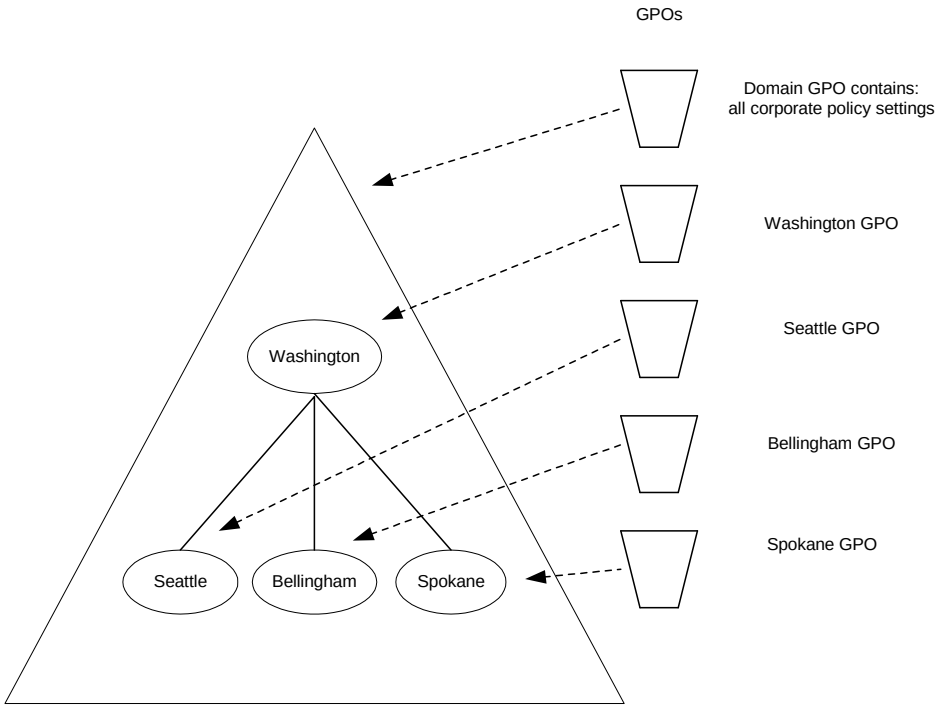


Layered GPO model

Monolithic GPO Design Model

The objective of this design is to create GPOs based on a monolithic design—an approach that reduces the number of GPOs 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.

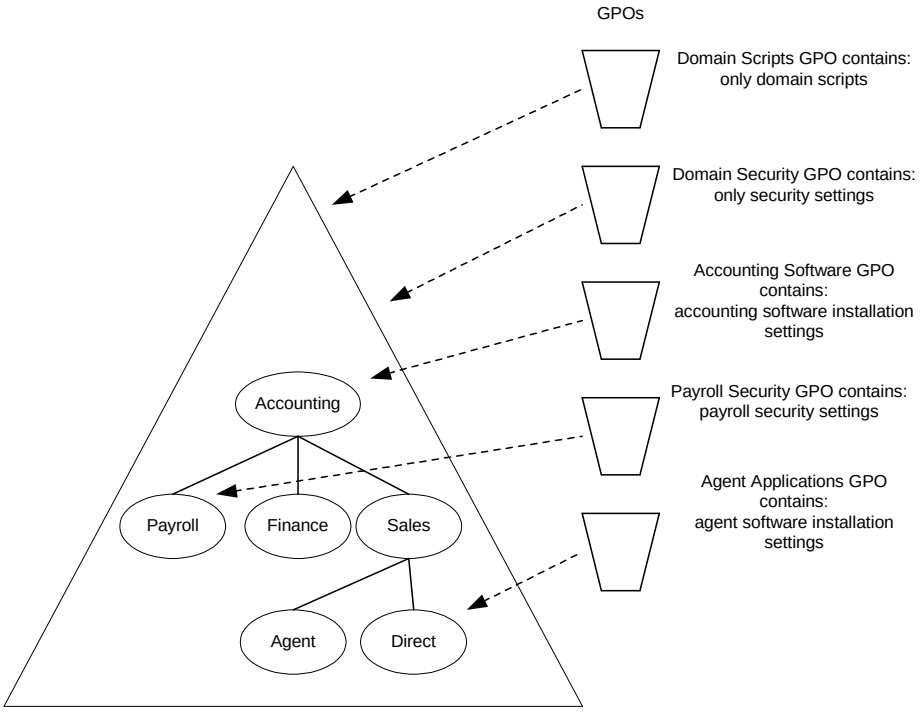


Monolithic GPO model

Single Policy Type GPO Design Model

The objective of this design is to create GPOs 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 GPO delivers only one type of policy (security GPOs 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.



Single Policy GPO Model

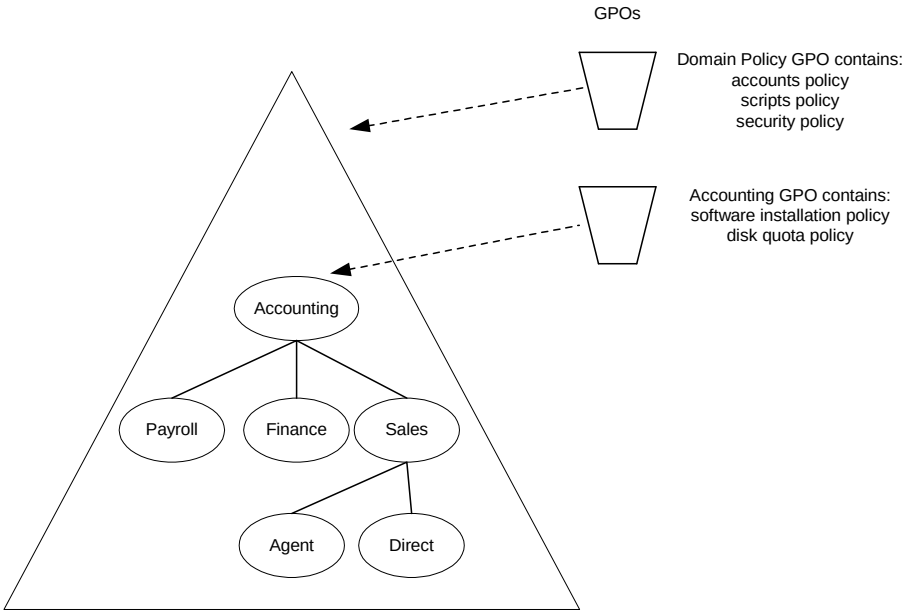
The following graphic illustrates an example of the single policy type GPO model.

Multiple Policy Types GPO Design Model

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

For example, you can create a GPO 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 GPO design that supports multiple policy types is useful in delegating administration environments and can reduce the number of GPOs that apply to a user and/or computer.

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

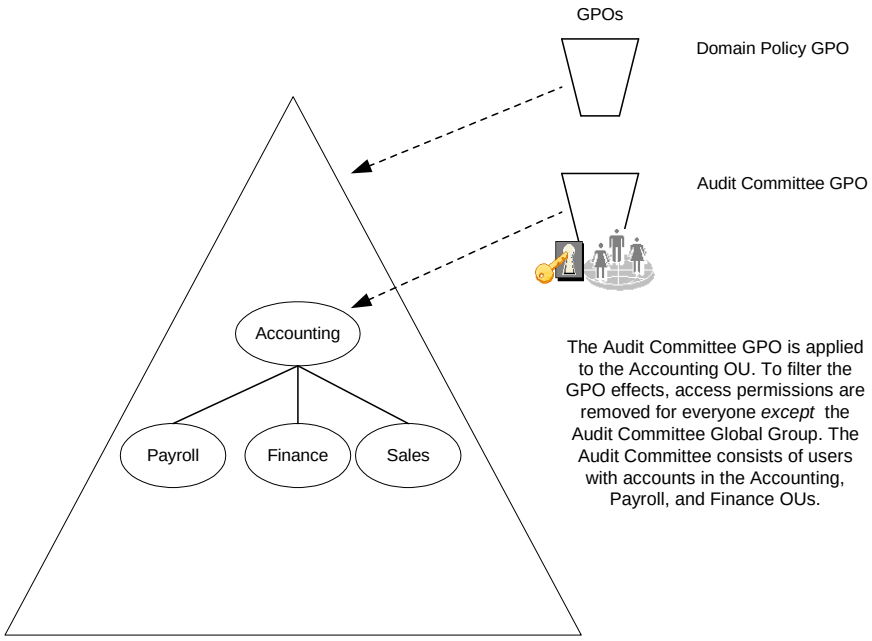


Multiple Policy Types GPO

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 organizational unit architecture does not reflect the team structure. This model works by using security filtering.

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



Team GPO Model

Public Computing Environment GPO Model

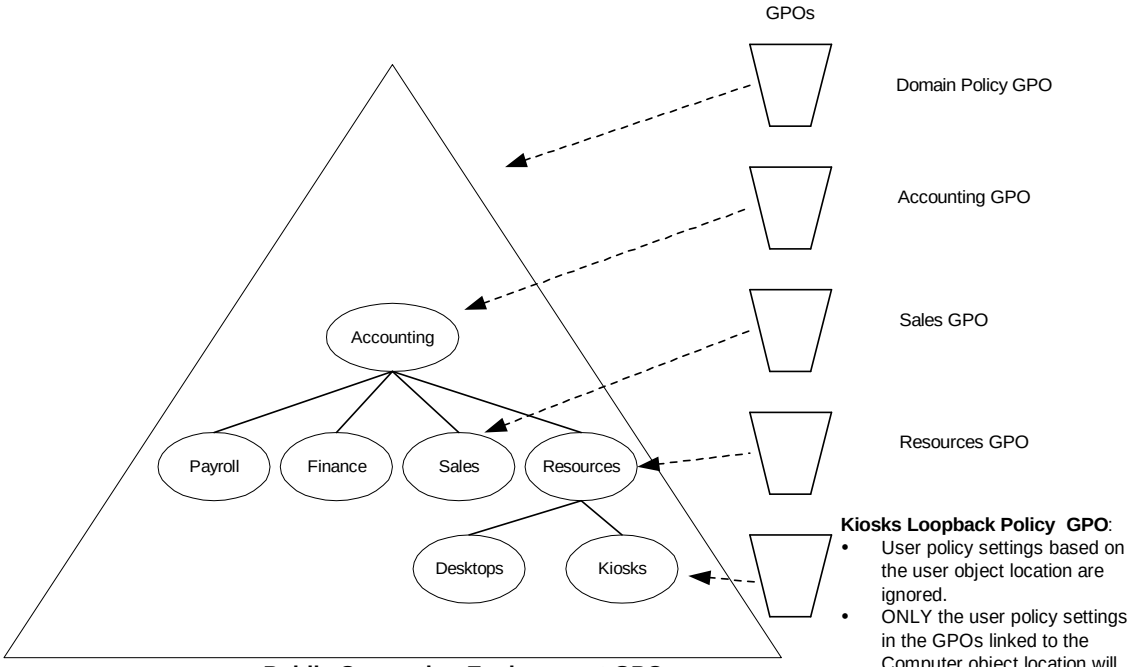
This scenario applies to environments were you want the computer Group Policy settings to always have precedence over the user Group Policy settings. This scenario is useful for training classes and kiosk-type environments in which you want to provide the same desktop environment regardless of which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

Normal Group Policy processing specifies that users in the Sales organizational unit get these GPOs: Domain Policy GPO, Accounting GPO, and Sales GPO. With the loopback policy enabled in **Replace mode**, when users from the Sales organizational unit log on to a computer in the Kiosks organizational unit, 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 organizational unit (and those inherited) are the *only* GPOs processed for the user logging onto computers in that organizational unit. Those in the Users organizational unit tree are not processed.

Delegation with Central Control

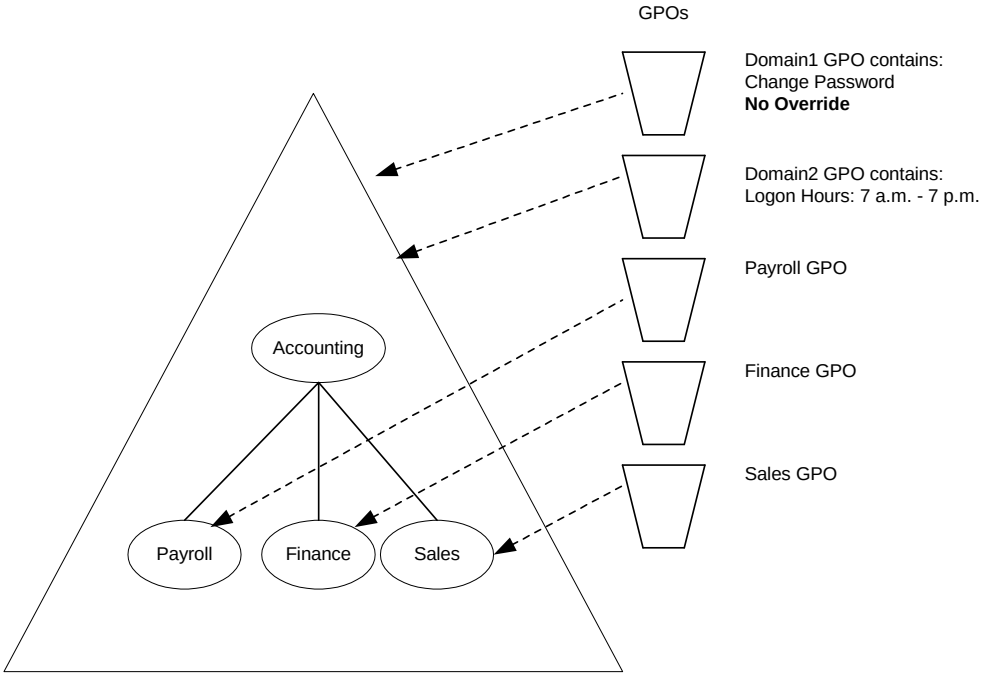
This model applies to organizations that choose to delegate administration of GPOs, but would like to enforce certain Group Policy settings throughout the domain (for example, specific security policy



Public Computing Environment GPO Model

settings).

The following graphic illustrates an example of GPO delegation with centralized control, and use of the



Delegation with central control

Enforce 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 organizational unit. Administrators of an organizational unit can block Group Policy settings that have been assigned at higher levels in the hierarchy from applying to his or her organizational unit. However, administrators cannot block Group Policy settings that are marked as Enforce.

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

Deployment Considerations

Administering a Mix of Windows 2000 and Windows Server 2003 Domains

GPMC exposes features that are available in the underlying operating system. Because new features have been added to Group Policy since Windows 2000, certain features will only be available in GPMC depending on the operating system that has been deployed on the domain controllers. This section describes these dependencies. In general, there are three key issues that determine whether a feature is available in GPMC:

- Whether the forest supports the Windows Server 2003 schema for Active Directory. Certain features are only available once the schema is upgraded. This is the first step that must be taken before any Windows Server 2003 domain controller can be deployed in an existing Windows 2000 forest. The schema is a forest-wide configuration and is upgraded by running **ADPrep /ForestPrep**. ADPrep is a utility included on the Windows Server 2003 CD. Note that it is possible to have the Windows Server 2003 schema in a forest with all Windows 2000 domain controllers.
- Whether there is at least one domain controller in the forest that is running Windows Server 2003. Group Policy Modeling must be performed on a domain controller running Windows Server 2003.
- Whether a domain contains the Windows Server 2003 domain configuration. This is implemented once **ADPrep /DomainPrep** is run in that domain. This is the first step that must be taken before any Windows Server 2003 domain controller can be deployed in an existing Windows 2000 domain.

Note that there is no dependency from the Group Policy perspective on whether a domain is in native mode or mixed mode.

Delegation of Group Policy Results and Group Policy Modeling

In order to delegate either Group Policy Modeling or Group Policy Results, the Active Directory schema in the forest must be the Windows Server 2003 schema. Note that you can use Group Policy Results even without this schema, but only users with local administrative credentials on the target computer can remotely access Group Policy Results data. Thus, if the forest does not have the Windows Server 2003 schema, the delegation pages in GPMC for organizational units and domains will not show these permissions.

Group Policy Modeling

Group Policy Modeling is a simulation that is performed by a service that can only run on a domain controller running Windows Server 2003 or later. As long as there is at least one domain controller running Windows Server 2003 in the forest, you can use Group Policy Modeling. GPMC will only show the Group Policy Modeling node in the user interface if the Windows Server 2003 schema is present.

WMI Filtering

WMI filters are only available in domains that have the Windows Server 2003 configuration. Although none of the domain controllers need to be running Windows Server 2003, you must have run ADPrep /DomainPrep in this domain. Also note that WMI filters are only evaluated by clients running Windows XP, Windows Server 2003, or later. WMI filters associated with a GPO will be ignored by Windows 2000 clients and the GPO will always be applied on Windows 2000.

If ADPrep /DomainPrep has not been run in a given domain, the WMI Filters node will not be present, and the GPO scope tab will not have a WMI filters section.

Upgrading Windows 2000 Domains to Windows Server 2003 Domains and Interaction with Group Policy Modeling

Group Policy Modeling is a new feature of Windows Server 2003 that simulates the resultant set of policy for a given configuration. The simulation is performed by a service that runs on Windows Server 2003 domain controllers. In order to perform the simulation in cross-domain scenarios, the service must have read access to all GPOs in the forest.

In a Windows Server 2003 domain (whether it is upgraded from Windows 2000 or installed as new), the Enterprise Domain Controllers group is automatically given read access to all newly created GPOs. This ensures that the service can read all GPOs in the forest.

However, if the domain was upgraded from Windows 2000, any existing GPOs that were created before the upgrade do not have read access for the Enterprise Domain Controllers group. When you click a GPO, GPMC detects this situation and notifies the user that Enterprise Domain Controllers do not have read access to all GPOs in this domain. To solve this problem, you can use one of the sample scripts provided with GPMC, GrantPermissionOnAllGPOs.wsf. This script can update the permissions for all GPOs in the domain. To use this script:

Ensure that the person running this script is either a Domain Admin or has permissions to modify security on all GPOs in the domain.

Open a command prompt and navigate to the **%programfiles%\gpmc\scripts** folder by typing:

```
CD /D %programfiles%\gpmc\scripts
```

Type the following:

```
Cscript GrantPermissionOnAllGPOs.wsf "Enterprise Domain Controllers"
/Permission:Read /Domain:value
```

The value of domain parameter is the DNS name of the domain.

Using Group Policy Features Across Forests

The Windows Server 2003 family introduces a new feature called Forest Trust that enables you to authenticate and authorize access to resources from separate, networked forests. With trusts established between forests, you can manage Group Policy throughout your enterprise, which provides greater flexibility especially in large organizations. This section describes Group Policy behavior in an environment with forest trust enabled:

- It is not possible to link a GPO to a domain in another forest.
- With Forest trust, it is possible that a user in Forest B could log onto a computer in Forest A. In this case, when the computer starts up, it will process policy for the computer configuration from Forest A, as usual. When a user from Forest B logs on, where they receive their policy settings from depends on the value of the **Allow Cross-Forest User Policy and Roaming Profiles** policy setting.
    - When this setting is **Not Configured**, no user-based policy settings are applied from the user's forest. Instead, loopback Group Policy processing will be applied, using the GPOs scoped to the computer. Users will receive a local profile instead of their roaming profile.

- When this setting is **Enabled**, the behavior is exactly the same as Windows 2000 Server: User policy is applied from the user's forest and a roaming user profile is allowed from the trusted forest.
- When this setting is **Disabled**, the behavior is the same as **Not Configured**.

This setting is available on Windows Server 2003 located at: Computer Configuration\Administrative Templates\System\Group Policy\Allow Cross-Forest User Policy and Roaming Profiles.

- It is possible to deploy Group Policy settings to users and computers in the same forest, but have those settings reference servers in other trusted forests. For example, the file shares that host software distribution points, redirected folders, logon scripts, and roaming user profiles could be in another trusted forest.
- Group Policy Modeling requires that both the user and the computer be in the same forest. If you want to simulate a user from Forest A logging on to a computer in Forest B, you must perform two separate Group Policy Modeling simulations: one for the user configuration and the other for the computer configuration.
- Delegation across forests is supported for managing Group Policy. For example, you can delegate to someone in Forest B the ability to perform Group Policy Modeling simulations on objects in Forest A.

Group Policy and Active Directory Sites

GPOs 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 GPO 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 GPO (and included policy settings), although the GPO 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 GPO across a WAN link.
- To manage site GPOs, you need to be either an Enterprise Admin or Domain Admin of the forest root domain.
- You may want to consider using site-wide GPOs for specifying policy for proxy settings and network-related settings.

In general, it is recommended that you link GPOs to domains and organizational units rather than sites.

Using Group Policy and Internet Explorer Enhanced Security Configuration

Windows Server 2003 includes a new default security configuration for Internet Explorer, called Internet Explorer Enhanced Security Configuration, also known as Internet Explorer hardening.

You can manage Internet Explorer Enhanced Security Configuration by:

- Enabling or disabling Internet Explorer Enhanced Security Configuration. This is commonly used in situations where you want to ensure that Internet Explorer Enhanced Security Configuration is always enabled. For example, Internet Explorer Enhanced Security Configuration might need to be reapplied on a specific computer if the local administrator on that computer disables it using the Optional Component Manager in the Windows Components Wizard (available from Add or Remove Programs.)

- Restricting who can manage trusted sites and other Internet Explorer security settings on a server. This is commonly used when you want to ensure that all servers have the same Internet Explorer Enhanced Security Configuration settings. For example, you might want to configure Internet Explorer Enhanced Security Configuration so that machined-based security settings are applied to each server rather than user-based security settings.
- Adding trusted Web sites and UNC paths to one of the trusted security zones. This is commonly used when you want to allow users access to specific Web sites and corporate resources, but still reduce the risk of users downloading or running malicious content.

Enhanced Security Configuration impacts the Security Zones and Privacy settings within the Internet Explorer Maintenance settings of a GPO. The Security Zones and Privacy settings can either be enabled with Enhanced Security Configuration or not.

When you edit settings for Security Zones and Privacy settings in a GPO from a computer where Enhanced Security Configuration is enabled, that GPO will contain Enhanced Security Configuration-enabled settings. When you look at the HTML report for that GPO, the Security Zones and Privacy heading will be appended with the text (Enhanced Security Configuration enabled).

When you edit settings for Security Zones and Privacy settings in a GPO from a computer where Enhanced Security Configuration is not enabled , that GPO will contain Enhanced Security Configuration-disabled settings. ESC is not enabled on any computer running Windows 2000 or Windows XP, nor on computers running Windows Server 2003 where ESC has been explicitly disabled.

Enhanced Security Configuration settings deployed through Group Policy will only be processed on and applied by computers where Enhanced Security Configuration is enabled. Enhanced Security Configuration settings will be ignored on computers where Enhanced Security Configuration is not enabled (all computers running Windows 2000 and Windows XP, and Windows Server 2003 computers where Enhanced Security Configuration has been explicitly disabled). The converse is also true: A GPO that contains non- Enhanced Security Configuration settings will only be processed on and applied by computers where Enhanced Security Configuration is not enabled.

For more information, see Managing Internet Explorer Enhanced Security Configuration, available from the Microsoft Group Policy Web site at http://www.microsoft.com/grouppolicy.

IntelliMirror Features without Active Directory

The full functionality of IntelliMirror® management technologies 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 clients running Windows 2000 or later:

- 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 the Microsoft IEAK Web site at 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 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.)

Setting Registry-based Policy in a Windows NT 4.0 Domain

A client running Windows 2000 or Windows XP Professional will process System Policy if either the user or computer account are in a Windows NT 4.0 domain. 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 file share of the authenticating Windows NT 4.0 domain controller.

Migrating Policy-Enabled Clients from Windows NT 4.0 to Windows 2000 or Windows Server 2003

This section discusses behavior of Group Policy and System Policy in relation to migration to Windows 2000 or Windows Server 2003.

Windows NT 4.0 and Windows 2000 Policy Setting Comparison

Group Policy differs greatly from System Policy in 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), System Policies:

- 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), as explained earlier in this paper 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 and Windows Server 2003, 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 linked to sites, domains, and organizational units.
- Affects all users and computers in the specified Active Directory container (site, domain, or organizational unit) by default.
- May be further controlled by user or computer membership in security groups.
- May be further controlled by use of WMI filtering.
- 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 2000Group Policy is that this does not occur. When a GPO no longer applies, registry settings written to the following secure registry locations are removed:

- HKLM\Software\Policies

- HKLM\Software\MS\Windows\CurrentVersion\Policies
- HKCU\Software\Policies
- HKCU\Software\MS\Windows\CurrentVersion\Policies

Migrating to Windows 2000 or Windows Server 2003

Migrating Windows NT 4.0-based clients and servers to Windows 2000 or Windows Server 2003 in various combinations causes different behavior for Group Policy. In a pure Windows 2000 or later environment where both the user and computer accounts are in a Windows 2000 or later domain, Windows 2000 or later clients process only Group Policy. System Policy is not processed. However, Windows 2000 or Windows XP clients can process System Policy in cases where either the user account and/or the computer account is not located in a Windows 2000 or Windows Server 2003 domain.

In many organizations it may be impractical to upgrade all Windows NT 4.0-based servers and client computers simultaneously to Windows Server 2003 and Windows XP. In this case, it is important that you know how 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 computers running Windows 2000 or later. There is no mechanism to process Group Policy on clients running Windows NT 4.0, Windows 95, Windows 98, and Windows Millennium Edition.

Upgrading Computer or User Accounts from Windows NT 4.0 to Windows Server 2003

When migrating from Windows NT 4.0, it's recommended to perform a clean installation of Windows Server 2003. To facilitate a clean installation, you can use the User State Migration Tool to migrate the users' data and settings to the new installation.

For more information about migrating from Windows NT 4 System Policy, see Windows 2000 Group Policy white paper at http://www.microsoft.com/windows2000/techinfo/howitworks/management/grouppolwp.asp.

Using Group Policy in a Mixed Environment of Windows 2000 and Windows XP Clients

Active Directory with Windows 2000 and Windows XP Clients

This section explains issues to consider when using Group Policy in a Windows 2000 Server or Windows Server 2003 environment where some or all of the clients are running Windows XP Professional or Windows 2000.

Comparing IntelliMirror Features on Windows 2000 and Windows XP

The following tables show how IntelliMirror features compare on computers running Windows 2000 Professional and Windows XP Professional.

Comparing Clients under Windows Server 2003 Active Directory

Feature	Supported in Windows 2000 Client	Supported in Windows XP Client
Group Policy	Yes	Yes
GPMC	No. But Windows 2000 clients can be managed with GPMC running on Windows Server 2003	Yes
Local Group Policy	Yes	Yes
System policy	Yes	Yes
Roaming profiles	Yes	Yes
Folder redirection	Yes (No home directory redirect)	Yes
Software installation	Yes	Yes
Internet Explorer Maintenance	Yes	Yes
Security Settings	Yes	Yes
Software restriction policies	No	Yes

Comparing clients under Windows 2000 Active Directory

Feature	Supported in Windows 2000	Supported in Windows XP
Group Policy	Yes	Yes
GPMC	No. But Windows 2000 clients in a Windows 2000 domain can be managed with GPMC installed on a computer running Windows XP or a member server running Windows Server 2003.	Yes
Local Group Policy	Yes	Yes
System policy	Yes	Yes
Roaming profiles	Yes	Yes
Folder redirection	Yes (No home directory redirect)	Yes
Software installation	Yes	Yes
Internet Explorer Maintenance	Yes	Yes
Security Settings	Yes	Yes
Software restriction policies	No	Yes (via Local Group Policy Object)

Comparing Clients Under Windows NT Server 4.0

Feature	Supported in Windows 2000	Supported in Windows XP
System policy	Yes	Yes
Group Policy	No	No
Local Group Policy	Yes	Yes
Roaming profiles	Yes	Yes
Folder redirection	No	No
Software installation	No	No
Internet Explorer Maintenance	Yes, with Internet Explorer Administration Kit (IEAK)	Yes, with IEAK.
Security Settings	No	No
Software restriction policies	No	No

Folder Redirection and Software Installation

Because background refresh is the default behavior in Windows XP, Folder Redirection and Software Installation may require as many as three logons to apply changes.

This behavior exists because Folder Redirection and Software Installation cannot apply during an asynchronous or background application of policy. Folder Redirection can only apply when processed synchronously.

Here is a sample scenario showing how polices are applied:

1. An administrator deploys a software package to User A.
2. User A logs on fast and receives a background (asynchronous) application of policy.
3. Because the policy application was asynchronous, the software that was set to be installed cannot be installed at this time. Instead the machine is tagged, indicating that software needs to be installed.
4. The next time the user logs on, the machine instead logs on the user synchronously to allow the software package to be installed. (This is the same behavior as Windows 2000). This results in one extra logon for the software to be installed.

In the case of Advanced folder redirection, because policy is evaluated based on security group membership three logons will be required: the first logon to update the cached user object (and security group membership), the second logon for policy to detect the change in security group membership and require a foreground policy application, and the third logon to actually apply folder redirection policy in the foreground.

Note When a client running Windows XP logs onto a Windows 2000 or Windows Server 2003 Active Directory, all Software Installation policy settings for Windows 2000 clients will be applied and work successfully on the Windows XP client.

Internet Explorer Maintenance

There are no changes in Internet Explorer Maintenance across Windows XP and Windows 2000.

Roaming Profiles

Users with roaming profiles can roam between Windows 2000 and Windows XP-based workstations without any changes in behavior. The new profile registry policy settings only work on Windows XP. If you apply these settings to a client running Windows 2000, they will have no effect.

Security Settings

Software Restrictions Policies were introduced in Windows XP. If you apply software restriction policy to a client running Windows 2000 it will have no effect. The software restriction policy registry settings will be written to the registry, but the Windows 2000 client will not know how to interpret them.

64 bit Integration Issues

If you apply a 64-bit package to Windows 2000 or a 32-bit version of Windows XP, it will not be advertised by default; however, you can override this behavior using the 64-bit deployment options in the Application Deployment Editor (ADE). If you apply a 64-bit package to a 64-bit version of Windows XP, it will be successfully advertised.

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 the Active Directory Installation Wizard. 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.

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 policy settings are always defined for the first domain controller of a Windows 2000 or Windows Server 2003 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 the Active Directory Installation Wizard. 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.

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 the Active Directory Installation Wizard, then they are removed: Backup Operators, Guests, Guest, and Users. If a Windows NT 4.0 domain controller is upgraded as the first Windows Server 2003 domain controller, 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 the Active Directory Installation Wizard, 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 the Active Directory Installation Wizard, 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 the Active Directory Installation Wizard, 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 the Active Directory Installation Wizard, 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 the Active Directory Installation Wizard, 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 policy settings in the past move to the new model of Group Policy for editing and configuring security policy settings.

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 policy settings 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 organizational units?

No. All domain controllers for a domain enforce the account policy settings that are defined in the Default Domain **Policy**. Domain controllers ignore password, lockout, or Kerberos policy settings defined at an organizational unit or Local GPO level.

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

The Group Policy model specifies that any policy settings configured locally may be overridden by like policy settings 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 policy settings to be applied to the local computer. To force a reapplication of policy to domain-level policy settings, 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 earlier 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 earlier APIs. When a user creates a computer account using this user right, the Domain Admins 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 and later, 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 GPMC. 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 Server 2003 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.

Appendix B: 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 is an Active Directory container that stores GPO 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 GPO is enabled or disabled.
- List of components (extensions) that have settings in the GPO.
- 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 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 policy settings, 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 GPO that you modified. For example, assume that you modified a GPO associated with a domain called Seattle. The resulting Group Policy template folder would be named as follows (the GUID is an example):

```
%systemroot%\sysvol\<SYSVOL>\Seattle.yourcompanyname.com\Policies\{47636445-af79-11d0-91fe-
080036644603}
```

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 Object Editor contain User or Computer data in the GPO.
- Whether the User or Computer portion is disabled.
- Version number of the Group Policy Object Editor 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 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.
  - **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 GPO.
  - Scripts\Logoff. Contains all the user logoff scripts and related files for this GPO.
- 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 GPO.

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 Unicode 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 Object Editor) to be applied to the Computer (**HKEY_LOCAL_MACHINE**) or User (**HKEY_CURRENT_USER**) 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.

When you use the Administrative Templates extension of the Group Policy Object Editor to define customized registry settings, 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 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 Object Editor, 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 Object Editor, 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 Object Editor, .adm file nodes are displayed. The .adm files within the Group Policy Object Editor 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 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 Object Editor, 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 Object Editor 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 policy settings, they reflect the current state.

Appendix C: WMI Filtering

How WMI Works

The WMI filters are evaluated on the client computer after the list of potential GPOs have been determined and filtered based on Security Group membership.

When a filter is applied to a GPO, it will be evaluated on the client computer. The GPO will only be applied if the entire query results in TRUE. Note that a GPO will be processed if no WMI filter has been selected.

During RSoP, in planning mode evaluation, a simulation of the client side processing occurs, producing a result based on the specified WMI Filters evaluation to TRUE.

For example:

- If no WMI filter is selected, all WMI filters are assumed to evaluate to true; therefore, all GPOs will apply.
- If a filter specified in the RSoP wizard matches a given GPO, the GPO will be evaluated.
- In the RSoP wizard, the wizard will show all the filters based on the list of GPOs that apply to a computer or user. If a filter is removed from the filter list, it is assumed to evaluate to false and the GPO that is associated with the filter will not apply.

Active Directory Schema additions

A new property called “gPCWQLFilter” has been added to the properties of a GPO. It includes the namespace path and GUID that represents the WMI filter.

Using WMI in Mixed Environments

Clients running Windows 2000 or earlier versions do not have support for WMI filters. They may however be affected by a GPO that has specified a WMI filter. In this case, the client will process the GPO as if the filter evaluated to TRUE because it has no way of knowing if it were FALSE.

However, a mixed environment supports the schema changes required to enable WMI filters. Windows Server 2003-based servers with WMI filter-enabled GPOs will continue to handle Windows 2000 clients as they did previously.

WMI filters are only available in domains that have at least one Windows Server 2003 domain controller. In an environment consisting only of Windows 2000 domains, the WMI filter node in GPMC is not shown.

Examples of WMI Filters

This section illustrates some scenarios in which administrators use WMI filtering to achieve a specific goal.

Software inventory-based targeting (Ored set)

A company purchases a site license for a new bounds-checker tool that helps software developers write more reliable code. Because the bounds-checker only works with Visual Basic®, Visual C, and Visual

C++,® the administrator wants to assign the package only on computers running any of these programs.

The administrator chooses the following filter:

Root\cimv2;Select * from Win32_Product where name = “MSIPackage1” OR name = “MSIPackage2” OR name = “MSIPackage32”

Note it may be more reliable to use IdentifyingNumber

Software inventory-based targeting(Anded set)

A software company discovers that the interaction of three software products causes instabilities on the system. The company develops a hot fix but only wants to install it on computers where this interaction is possible.

The administrator chooses the following filter:

root\cimv2;Select * from Win32_Product where name = “MSIpackage1“

root\cimv2;Select * from Win32_Product where name = “MSIPackage2”

root\cimv2;Select * from Win32_Product where name = “MSIPackage3”

Note it may be more reliable to use IdentifyingNumber.

Operating system-based targeting

An administrator wants to deploy an enterprise monitoring policy but needs to limit the target set to computers running either Windows 2000 Server or Advanced Server.

The administrator chooses the following filter:

Root\CimV2; Select * from Win32_OperatingSystem where Caption = “Microsoft Windows 2000 Advanced Server” OR Caption = “Microsoft Windows 2000 Server”

Hardware inventory-based targeting

An administrator wants to deploy a new connection-manager but needs to avoid wasting space on desktop computers without modems where the connection manager would be useless. An administrator can deploy the package across the enterprise with the following WMI-filter:

Root\CimV2;Select * from Win32_POTSModem

Resource-based targeting

To encourage field engineers and consultants to use documentation, a company wants to make Help systems available directly on users’ hard disks. But because users complain that the Help files consume too much space, a manager decides to only deploy the documentation on computers that have at least 600 megabytes (MB) available.

An administrator can accomplish this with the following WMI filter:

Root\CimV2; Select * from Win32_LogicalDisk where FreeSpace > 629145600 AND Description <> “Network Connection”

Computer-based targeting

An administrator wants to set up a policy to encrypt all “My Documents” folders on notebook computers. The administrator determines that all the company’s notebook computers are Toshiba Tecra models 800 and 810.

To set up the policy, an administrator uses the following WMI filter:

Root\CimV2; Select * from Win32_ComputerSystem where manufacturer = “Toshiba” and Model = “Tecra 800” OR Model = “Tecra 810”

Asset tag-based targeting

An administrator wants to set hardware inventory monitoring policy for all computers with an “asset tag” of 300,000-355555.

To set up the policy, an administrator uses the following WMI filter:

Root\Cimv2 ; Select * from Win32_SystemEnclosure where SMBIOSAssetTag > ‘300000’ AND SMBIOSAssetTag < ‘355555’

Hardware configuration-based targeting

An administrator wants to target a policy for all computers that have a network adapter on interrupt number 11. The administrator chooses the following filter:

Root\cimv2; Associators of {win32_IRQResource.IRQNumber=11} where resultclass = Win32_NetworkAdapter

Configuration-based targeting

An administrator wants to avoid turning on “netmon” on computers enabled with multicasting turned on. The administrator chooses the following filter:

Select * from Win32_NetworkProtocol where SupportsMulticasting = true

File attribute-based targeting

An administrator only wants to disable sharing of folders on systems where at least one of “My Documents” directories are not encrypted. The administrator chooses the following filter:

Root\cimv2 ; Select * from Win32_Directory where filename =’my documents’ AND encrypted = false

Time zone-based targeting

An administrator needs to target a policy on all servers located on the East Coast of the United States. The administrator chooses the following filter:

Root\cimv2 ; Select * from win32_timezone where bias =-300

Hot fix-based targeting

An administrator only wants to apply a policy on computers that have a specific hot fix or QFE. The administrator chooses the following filter:

Root\cimv2 ; select * from Win32_QuickFixEngineering where HotFixID = ‘q147222’

Further Information

The WMI SDK has a tool called cimstudio. This allows users to find a class, searching by name, description, property name, and so forth. Users can then experiment with queries on the class and optimize it before creating a new filter. For more information, see Windows Management Instrumentation in the Microsoft Platform SDK at http://msdn.microsoft.com/library/default.asp?url=/library/en-us/wmisdk/wmi/wmi_start_page.asp.

Appendix D: 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 policy settings?

You cannot set up any Group Policy directly on a computer or user object; a GPO 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 organizational unit, you can use WMI or security filtering.

For information on filtering, see the section earlier in this document, Filtering the Scope of the Group Policy Object.

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

Group Policy is processed in the following order: Local GPO, site, domain, organizational unit, and additional child organizational units. This means that the Local GPO is processed first, and the organizational unit 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 GPO (not local GPO) may be enforced by using the **Enforce** option so that its policy settings cannot be overwritten. When more than one GPO has been marked as enforced, the GPO that is highest in Active Directory hierarchy takes precedence.
- At any site, domain, or organizational unit, Group Policy inheritance may be selectively designated as Block Inheritance. However, blocking inheritance does not prevent policy from **enforced** GPOs from applying; this is because enforced GPOs are always applied, and cannot be blocked.

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

No, GPOs are applied only to the users and computers that are members of the organizational unit.

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 organizational unit. However, you can filter the scope of a GPO in one of two ways by using WMI filtering or security filtering based on membership of those users in a security group, by adjusting the 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 organizational unit 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 information on filtering, see the section earlier in this document, Filtering the Scope of the Group Policy Object.

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 in not available. You may cancel this operation for this session or retry using one of the Following domain controller choices."?

The Group Policy Object Editor uses the primary domain controller emulator Operations Master token when editing a GPO. For information, see Group Policy Replication and Domain Controller Selection, and Group Policy Object Editor and the Operations Master earlier in this paper.

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

Use the copy feature in GPMC. A copy operation allows you to transfer settings from an existing GPO in Active Directory directly into a new GPO. The new GPO created during the copy operation is given a new GUID and is unlinked. You can use a copy operation to transfer settings to a new GPO in the same domain, another domain in the same forest, or a domain in another forest. Because a copy operation uses an existing GPO in Active Directory as its source, trust is required between the source and destination domains. Copy operations are suited for moving Group Policy between production environments, and for migrating Group Policy that has been tested in a test domain or forest to a production environment, as long as there is trust between the source and destination domains. For more information and step-by-step instructions, see GPMC Help.

Infrastructure - Client side

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 policy settings 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, organizational unit, and so on. The UI is displayed while policy settings are being processed.

Note Windows NT 4.0 style policy settings process both computer and user settings, potentially overwriting 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 policy settings.

By default in Windows XP Professional, the Fast Logon Optimization feature is set for both domain and workgroup members. This results in the asynchronous application of policies when the computer starts and when the user logs on. For more information, see Fast Logon in Windows XP Professional earlier in this paper.

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 Object Editor.

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 Policy settings?

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

Which policy settings do I see when viewing the policy settings that are set when the Group Policy Object Editor is run focused on a local computer?

This shows the information in the Local GPO, 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 organizational unit).

Tools

What is the purpose of the various Group Policy tools available from Microsoft?

- Group Policy Management Console. A new MMC console to view and edit Group Policy properties, generate reports, copy, import, backup, restore, and to select GPOs for editing. GPMC is designed to be the single place where you can view and manage GPOs in multiple forests and domains.
- Active Directory Users and Computers. An MMC console to view and edit Group Policy properties and to select GPOs for editing. Note: Most functionality in this snap-in is now contained in GPMC.
- Group Policy Object Editor. An MMC console for editing Group Policy settings. It is launched from GPMC; for example, by right-clicking a GPO in the tree view and choosing Edit.
- Active Directory Sites and Services. An MMC console to force replication.
- Resultant Set of Policies. An MMC snap-in to view a detailed analysis of Group Policy settings for the local computer. Note: RSoP functionality is now optimized in GPMC as Group Policy Results and Group Policy Modeling. It is used with GPMC to provide precedence information.
- Secedit. A command-line tool that configures and analyzes system security by comparing your current configuration to at least one template. Note: Secedit\refreshpolicy does not work on Windows XP and later; use Gpupdate instead.
- Gpupdate. On Windows XP and Windows Server 2003, a command-line tool that refreshes local Group Policy settings and Group Policy settings that are stored in Active Directory, including security settings. This tool replaces Secedit on Windows XP and Windows Server 2003.
- Local Security Policy. An MMC snap-in to verify local security settings.
- dcdiag /v and netdiag /v. Command-line tools that use the verbose option to test DNS on each domain Controller and review the output to verify DNS name resolution.
- nslookup and netdiag /v. Command-line tools that use the verbose option to test DNS on member servers to verify that DNS is working.
- Repadmin. A command-line tool that you can use to determine the directory replication partners of the destination server, and then issue a command to synchronize the source server with the destination server.
- Gpresult. A command-line tool to display the policies applied to the local computer.
- Gpotool. A command line tool to check the health of the GPOs on domain controllers.

Group Policy Management Console

Where can I download the Group Policy Management Console?

GPMC is available from the Microsoft GPMC home page at http://www.microsoft.com/windows.netserver/gpmc/.

What are the system requirements for GPMC?

GPMC can manage both Windows 2000 and Windows Server 2003 domains with Active Directory service. In either case, the computer on which the tool itself runs must be running Windows Server 2003 or Windows XP Professional (with Windows XP Service Pack 1 and the Microsoft .NET

Framework). Note: When installing GPMC on Windows XP Professional with SP1, a post SP1 hotfix is required. This hotfix (Q326469) is included with GPMC. GPMC Setup prompts you to install Windows XP QFE Q326469 if it is not already present.

Is it necessary to install GPMC on a domain controller?

GPMC can be installed on any computer that belongs to the domain as long as it is running Windows Server 2003 or Windows XP Professional in accordance with the system requirements explained earlier.

Can the Group Policy Management Console be run through a Terminal Services session?

Yes, GPMC should work reliably via Terminal Services or local consoles.

How can you compare the settings contained within two GPOs?

Microsoft doesn't currently provide any tools that allow you to easily compare two or more Group Policy settings. However, in GPMC, you can generate an XML report from Group Policy Results and then compare the reports for the GPOs.

Group Policy Object Editor

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

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

- 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.

Uncheck the filtering Only show policy settings that can be fully managed in the Group Policy Object Editor using the following procedure: right click any administrative template node and select View and then click Filtering. In the Filtering dialog box, clear the check box for Only show policy settings that can be fully managed and click OK.

General Issues

Can I transfer System Policies to Group Policy Objects?

You cannot migrate Windows NT 4.0 System Policies *directly* to Windows Server 2003. 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 Server GPO structure. For more information, see How to Use the Group Policy Migration Utility to Migrate Windows NT System Policy Settings at http://support.microsoft.com/default.aspx?scid=kb;en-us;317367.

With Windows 2000 or later, when a Windows NT 4.0 client is upgraded to Windows 2000 or Windows XP, it will get only Active Directory-based Group Policy settings and not Windows NT 4.0-style policy settings.

Do Group Policy settings override User Profile settings?

Yes.

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

Although scripted control of individual settings inside a GPO is not provided, GPMC provides a comprehensive set of COM interfaces for scripting many Group Policy-related operations. The interfaces are documented in the Group Policy Management Console SDK, which is located at **%programfiles%\gpmc\scripts\gpmc.chm** on any computer where you installed GPMC.

When you install GPMC, a set of sample scripts illustrating the use of these interfaces are installed to the **%programfiles%\gpmc\scripts** directory.

The sample scripts address real-world administrative problems and scenarios. You can perform various tasks such as finding all GPOs in a domain that have duplicate names or generating a list of all GPOs in a domain whose settings are disabled or partially disabled.

Glossary

This section presents terminology used in this document.

Active Directory

The Windows 2000 Server and Windows Server 2003 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 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 4.0, and Windows 95, Windows 98, and Windows Millennium Edition operating system and registry structure. The .adm file specifies the registry settings that can be modified through the Group Policy Object Editor 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 Object Editor 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 Object Editor 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

You can assign applications to either a user or a computer using Group Policy. When you assign applications to a computer, the application is automatically installed the next time the computer is started. When you assign applications to a user with Group Policy, the administrator can choose to either have the application installed on-demand when the user selects the application or in-full when the user next logs on:

- On Demand. If the application is installed on demand, the user's computer is set up with a Start menu shortcut, and the appropriate file associations are created in the registry. To the user, it looks and feels as if the application is already present. However, the application is not fully installed until the user needs the application. When the user attempts to open the application or a file associated with that application, Windows Installer checks to make sure that all the files and parameters of the application are present for the application to properly execute. If they are not present, Windows Installer retrieves and installs them from a predetermined distribution point. Once in place, the application opens.
- Full Install. The full-install option is useful for specific groups of users such as frequent travelers who might require all available applications to be fully installed before they travel. With full install, a user’s applications are installed at logon.

application publishing

In Windows 2000 and Windows Server 2003, you can use the Software Installation snap-in extension of the Group Policy Object Editor 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 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 Active Directory, users can activate it by document association, just as an assigned application. Users can also set up the program using the Add or 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 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 Object Editor 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 stres only the information about the objects located in that domain. By partitioning the directory information this way, Active Directory scales up to as many objects as you need to store information about on your network.
- The administraor of a domain has absolute rights to set policy settings 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 Object Editor extension that you use to place the Windows 2000 or Windows Server 2003 special folders in network locations other than their default location

(%systemroot%\Documents and Settings\%userprofile%) 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 and Windows Server 2003 to define options for managed desktop configurations for groups of users and computers. To specify Group Policy options, you use GPMC in conjunction with the Group Policy Object Editor.

Group Policy engine

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

Group Policy Management Console (GPMC)

An MMC console to view and edit Group Policy properties, generate reports, copy, import, backup, restore, and to select GPOs for editing. GPMC lets administrators manage Group Policy for multiple domains and sites within a given forest, all in a simplified user interface with drag-and-drop support. Operations are fully scriptable, which lets administrators customize and automate management.

Group Policy object

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

Group Policy Object Editor

To edit a specific desktop configuration for a particular group of users and computers, you use the Group Policy Object Editor, also known previously as the Group Policy snap-in, Group Policy Object Editor, or GPedit.

You can specify Group Policy settings for the following:

- Registry-based policy settings—Includes Group Policy for the Windows 2000 and Windows Server 2003 operating systems and their components and for applications. To manage these settings, use the Administrative Templates node of the Group Policy Object Editor.
- 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- and Windows Server 2003-based computers.
- Remote Installation Services—Used to control the behavior of the Remote Operating System Installation feature as displayed to client computers

Group Policy Modeling

This is a simulation of what would happen under circumstances specified by an administrator. Group Policy Modeling requires that you have at least one domain controller running Windows Server 2003 because this simulation is performed by a service running on a domain controller that is running Windows Server 2003. With Group Policy Modeling, you can either simulate the RSoP data that would be applied for an existing configuration, or you can perform "what-if" analyses by simulating hypothetical changes to your directory environment and then calculating the RSoP for that hypothetical configuration. For example, you can simulate changes to security group membership, or changes to the location of the user or computer object in Active Directory. Outside of GPMC, Group Policy Modeling is referred to as RSoP - planning mode.

Group Policy Results

This represents the actual policy data that is applied to a given computer and user. It is obtained by querying the target computer and retrieving the RSoP data that was applied to that computer. The Group Policy Results capability is provided by the client operating system and requires Windows XP, Windows Server 2003 or later. Outside of GPMC, Group Policy Results is referred to as RSoP - logging mode.

IntelliMirror

IntelliMirror refers to the ability to provide users with consistent access to their applications, application settings, roaming user profiles, and user data, from any managed computer—even when they are disconnected from the network. IntelliMirror is delivered via a set of Windows features that enable IT administrators to implement standard computing environments for groups of users and computers. IntelliMirror can significantly boost user productivity and satisfaction by doing the following:

- Allowing users to continue working efficiently in intermittently connected or disconnected scenarios by enabling uninterrupted access to user and configuration data under these conditions.
- Delivering a consistent computing environment to users from any computer when their desktop or laptop computer is unavailable or in scenarios where users are not assigned a specific computer.
- Minimizing data loss by enabling centralized backup of user data and configuration files by the IT organization.
- Minimizing user downtime by enabling automated installation and repair of applications.
- Implementing IntelliMirror also boosts administrator efficiency and reduces IT costs by doing the following:
- Eliminating the need to manually configure user settings, install applications, or transfer user files to provide users access to their computing environments on any computer.
- Enabling scenarios where users don’t have an assigned computer but log in to any available computer in a pool of computers. This helps reduce hardware and administration costs.
- Easing the IT task of implementing centralized backup of user files while satisfying need for these files to be available on the user’s computer.
- Reducing support costs by using Windows Installer to automatically repair broken application installations.

- IntelliMirror is implemented by means of a set of Windows features, including Active Directory, Group Policy, Software Installation, Windows Installer, Folder Redirection, Offline Folders, and Roaming User Profiles.

Internet Explorer Maintenance

A Group Policy extension snap-in that includes policy settings to manage the following: Browser User Interface, Connection Settings, Custom URLs, Security, and Program Associations.

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. MMC console hosts the administrative tools (these are called MMC snap-ins); the console itself provides no management functionality.

Migration table

A migration table is a file that maps references to users, groups, computers, and UNC paths in the source GPO to new values in the destination GPO. A migration table consists of one or more mapping entries. Each mapping entry consists of a type, source reference, and destination reference. If you specify a migration table when performing an import or copy, each reference to the source entry will be replaced with the destination entry when writing the settings into the destination GPO. Migration tables store the mapping information as XML, and have their own file name extension, .migtable. You can create migration tables using the Migration Table Editor (MTE). The MTE is a convenient tool for viewing and editing migration tables without having to work in, or be familiar with, XML. The MTE is associated with the .migtable extension so that when you double click a migration table, it opens in the MTE. The MTE is installed with GPMC.

MMC snap-in

Tools that extend 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 (organizational unit)

A type of directory object contained within domains. organizational units 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 component that administrators can use to remotely install a local copy of the Windows 2000 Professional or Windows XP Professional 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 operating system Installation Group Policy settings that administrators define for the site, domain, or organizational unit to which the users belong, in conjunction with the specific security group or user account.

Resultant Set of Policy (RSoP)

RSoP allows administrators to see the effect of Group Policy on a targeted user or computer. RSoP is an infrastructure leveraged by GPMC to enable Group Policy Results and Group Policy Modeling. In Group Policy Results, administrators assess what has applied to a particular target. In Group Policy Modeling, administrators can see how policy settings would be applied to a target and then examine the results before deploying a change to Group Policy.

Roaming user profile

A copy of the local user profile stored on a server share. This profile is downloaded every time that a user logs on to any computer on the network, and any changes made to a roaming user profile are synchronized with the server copy upon logoff. See also user profile.

schema

The formal definition of all object classes, and the attributes that make up those object classes, that can be stored in the directory. Active Directory includes a default schema, which defines many object classes, such as users, groups, computers, domains, organizational units, and security policy settings. 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 and Windows Server 2003 support Windows Script Host Visual Basic Scripting 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 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 GPO. A security configuration consists of settings applied to each security area supported for Windows 2000 or Windows XP Professional and Windows 2000 Server and Windows Server 2003. This configuration is included within a GPO.

site

In Windows 2000 and Windows Server 2003 you register your network's physical topology by defining sites. A site is defined as one or more IP subnets. Windows 2000 and Windows Server 2003 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, 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.

tattooing

This refers to a registry setting that is set using Windows NT 4.0 System Policies, the setting persists until the specified policy is reversed or the user edits the registry.

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.

user profile

A user profile describes the desktop computing configuration for a specific user, including the user's environment and preference settings. A profile is created the first time that a user logs on to a computer running Windows Server 2003, Windows XP, Windows 2000, or Windows NT Workstation. A user profile is a group of settings and files that defines the environment that the system loads when a user logs on. It includes all the user-specific configuration settings, such as program items, screen colors, network connections, printer connections, mouse settings, and window size and position. Profiles are not user policies and the user has a profile even if you don't use Group Policy.

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 Object Editor uses .msi packages.

Windows Management Instrumentation (WMI)

A management infrastructure that supports monitoring and controlling system resources through a common set of interfaces and provides a logically organized, consistent model of Windows operation, configuration, and status. WMI Filtering in Windows Server 2003 allows you to create queries based on this data. These queries (also called WMI filters) determine which users and computers receive all of the policy configured in the GPO where you create the filter.

Related Links

- Microsoft.com Group Policy Home Page at http://www.microsoft.com/grouppolicy. Provides an entry point for Group Policy documentation on the Web. Includes links to documentation, knowledge base articles, support information, and newsgroups.
- Windows Server 2003 Deployment Kit, Designing a Managed Environment. at http://www.microsoft.com/grouppolicy. Available from the Microsoft Group Policy home page, this book describes the technologies in Windows Server 2003 associated with deployment of a managed environment. Has significant coverage of Group Policy and related IntelliMirror technologies. Includes planning, designing, and implementation guidance.
- Troubleshooting Windows Server 2003 Group Policy. at http://www.microsoft.com/grouppolicy. Available from the Microsoft Group Policy home page, this white paper provides a structured guide to troubleshooting Group Policy operations. Covers Group Policy processing itself, dependent technologies and relevant troubleshooting tools.
- Group Policy Administration using the Group Policy Management Console. at http://go.microsoft.com/fwlink/?LinkID=14320. This white paper provides technical details of functionality in GPMC.
- Migrating GPOs Across Domains with GPMC. at http://go.microsoft.com/fwlink/?LinkID=14321. This white paper explains how to migrate GPOs from one domain to another using GPMC.
- **Group Policy Management Console Software Development Kit (SDK).** Provides information about how to use the COM interfaces of Group Policy Management, which support scripting many of the operations supported by Group Policy Management Console. This is available when you install GPMC. See "gpmc.chm" in the **%programfiles%\gpmc\scripts** directory. The SDK is only available in English.

Feedback on this Paper

If you have any comments about this paper, contact mailto:gpdocs@microsoft.com.

Newsgroups About Group Policy

If you have a question about Group Policy, you can post to the newsgroup “microsoft.public.windows.group_policy.”