

Bulletproof Your Windows Network with Group Policy

written by
Darren Mar-Elia
Chief Technology Officer
Windows Management
Quest Software, Inc.

White Paper

Abstract

The Group Policy feature in Windows 2000, Windows XP, and Windows Server 2003 provides powerful capabilities for automatically managing and configuring servers and workstations in large, distributed Windows environments. Group Policy features let administrators globally set system security, lock down desktop settings to reduce user errors, redirect user folders, distribute software, control Internet Explorer (IE) configuration, and a variety of other policy settings.

Unfortunately, the complexity of Group Policy, with all of its available policy options, has a tendency to discourage enterprises from taking full advantage of this powerful technology. This paper discusses the architecture and function of Group Policy and how to optimize it to fortify the security and usability of your environment.

Copyright © 2004 Quest Software, Inc. and Quest are registered trademarks of Quest Software. The information in this publication is furnished for information use only, does not constitute a commitment from Quest Software Inc. of any features or functions discussed and is subject to change without notice. Quest Software, Inc. assumes no responsibility or liability for any errors or inaccuracies that may appear in this publication.

Last revised October 6, 2004

QUEST SOFTWARE **Windows Management**

6500 Emerald Parkway
Suite 400
Columbus, OH 43016, USA

Phone: 614-336-9223
1-800-263-0036

URL: www.quest.com/microsoft

CONTENTS

INTRODUCTION	5
UNDERSTANDING GPO STRUCTURE AND FUNCTION.....	6
GPO STRUCTURE	6
<i>The Group Policy Container and Group Policy Template</i>	<i>7</i>
<i>GPO Versioning.....</i>	<i>9</i>
GPO PROCESSING	9
<i>GPO Linking.....</i>	<i>9</i>
<i>LSDOU Processing Order and Resultant Set of Policy.....</i>	<i>11</i>
<i>No Override and Block Inheritance.....</i>	<i>12</i>
<i>Security Group Filtering.....</i>	<i>13</i>
<i>The Client's Role in Processing.....</i>	<i>15</i>
<i>Background Processing.....</i>	<i>17</i>
UNDERSTANDING WHAT GROUP POLICY CAN DO.....	19
OVERVIEW OF POLICY FUNCTIONALITY.....	19
SOFTWARE INSTALLATION.....	21
SCRIPTS	23
SECURITY	23
ADMINISTRATIVE TEMPLATES	25
REMOTE INSTALLATION SERVICES POLICY	26
FOLDER REDIRECTION.....	26
INTERNET EXPLORER MAINTENANCE	27
DESIGNING A BULLETPROOF GROUP POLICY IMPLEMENTATION ...	28
ACTIVE DIRECTORY NAMESPACE PLANNING AND GROUP POLICY	28
<i>Where Do I Link My GPOs?.....</i>	<i>29</i>
<i>How Monolithic Should My GPOs Be?.....</i>	<i>31</i>
BEST PRACTICES FOR SECURITY POLICY	33
BEST PRACTICES FOR AT POLICY.....	34
BEST PRACTICES FOR OTHER AREAS OF GROUP POLICY.....	35
CONCLUSION	36
ABOUT THE AUTHOR	37
ABOUT QUEST WINDOWS MANAGEMENT.....	38
ABOUT QUEST SOFTWARE, INC.	38

INTRODUCTION

Group Policy is a key feature in Windows 2000 and Windows Server 2003 for managing Microsoft Active Directory (AD) infrastructures. Group Policy can significantly reduce the costs of deploying and maintaining Windows in the enterprise because it lets an administrator simultaneously effect configuration changes on thousands of workstations and servers within an AD infrastructure. But the potential return on investment in Group Policy will not be realized if the complexity of managing policy requires spending more rather than less time administering Windows.

Unfortunately, complexity arising from the myriad of policy configuration options within GPO can quickly outstrip the intended benefit. To take full advantage of Group Policy requires proper knowledge of best practices to ensure consistent, expected application of policy. This paper provides those best practices.

UNDERSTANDING GPO STRUCTURE AND FUNCTION

Taking full advantage of Group Policy requires that Active Directory be deployed. However, every Windows 2000, XP, and Windows Server 2003 device does come with a local GPO that contains a subset of the available policy functionality. You can view and edit the local GPO using the Microsoft Management Console (MMC) Group Policy Editor snap-in tool, or by simply typing “gpedit.msc” from the Start | Run dialog.

GPO Structure

Figure 1 shows what a local GPO looks like on Windows XP.

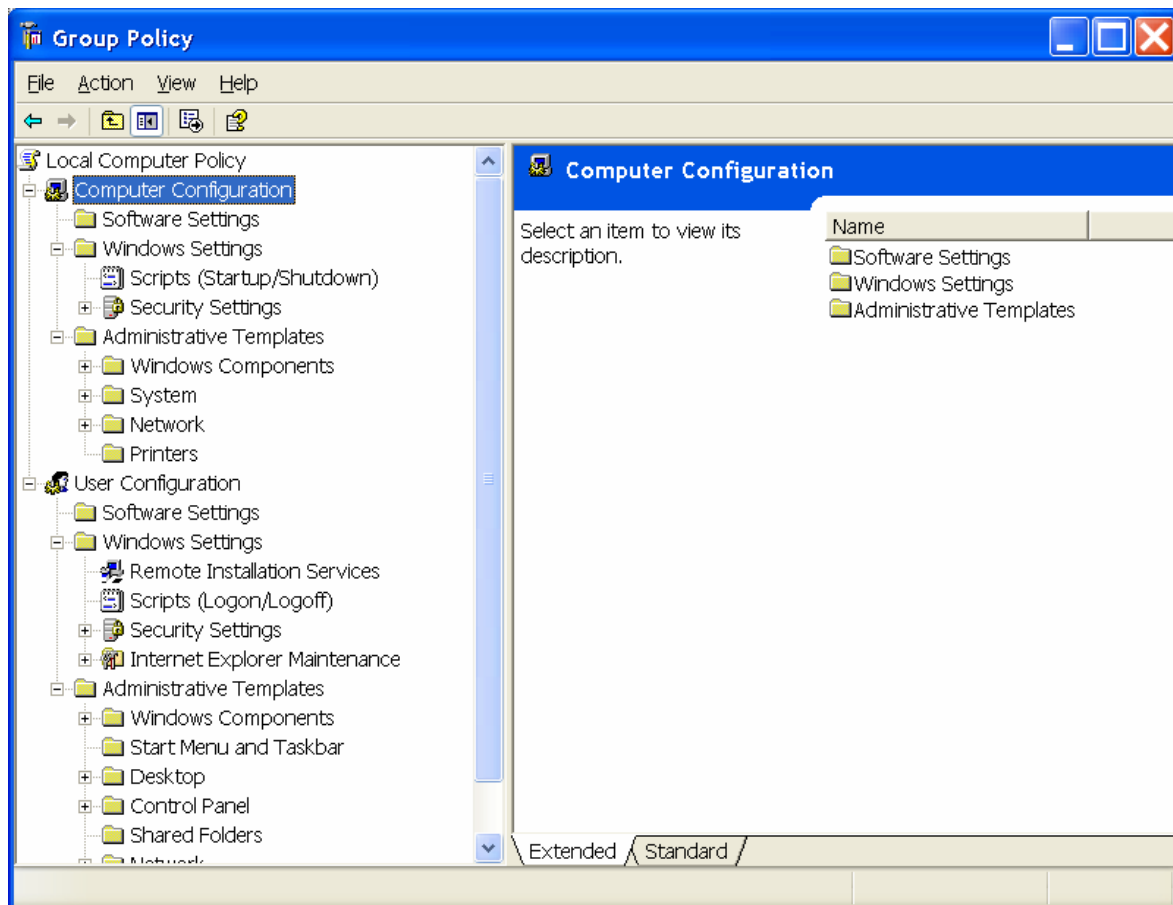


Figure 1: Viewing the local GPO in the MMC Group Policy snap-in.

As Figure 1 illustrates, a GPO has two types of settings: Computer Configuration and User Configuration. The Computer Configuration part controls settings that apply to a computer regardless of who is logged on to that computer. User Configuration policy is applied to users who are logging on to Windows computers. Therefore, Computer Configuration settings are processed only when the computer is booted up (or shut down), while User Configuration settings apply only when a user logs on (or logs off) the computer.

The Group Policy Container and Group Policy Template

A GPO is composed of two parts: the Group Policy Container (GPC) and the Group Policy Template (GPT). The GPC is stored in Active Directory and contains general information about the GPO, such as its version number, Lightweight Directory Access Protocol (LDAP) path, creation date and time, and last modified date and time. The GPC also contains objects related to the Software Installation feature within Group Policy. These objects, called the Class Store, define details about the software application deployed. A GPC is located within each AD domain in the System\Policies container. Figure 2 shows where to find the GPC within AD using the AD Users and Computers MMC snap-in in Advanced View.

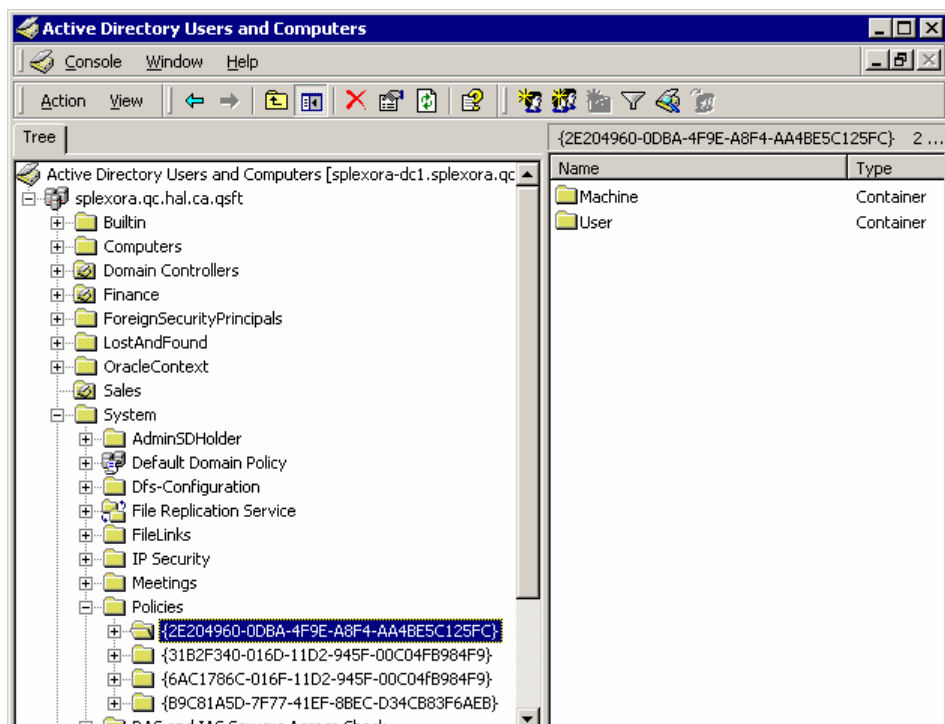


Figure 2: Viewing the GPC within an Active Directory domain.

The highlighted container in Figure 2 represents a GPO, as shown by its Globally Unique ID (GUID). Each GPO defined in a domain has a folder in this Policies container. In the right-hand results pane, there are two subfolders under the main folder: “Machine” and “User.” These represent the two “sides” to a GPO, and they contain the Class Store information.

The other part of a GPO, the GPT, is a set of folders within the SYSVOL share, located on every domain controller (DC) within an AD domain. The SYSVOL share is a part of the file system replicated automatically to all DCs by the NT File Replication Service (NTFRS). Under the SYSVOL share is a folder named according to the DNS domain name that the DC is a member of. Underneath this domain-named folder is a folder called “Policies,” and within this folder are a number of GUID-named subfolders (see Figure 3) that correspond to each GPO defined in the domain. These are the same GUIDs shown in Figure 2 within the GPC.

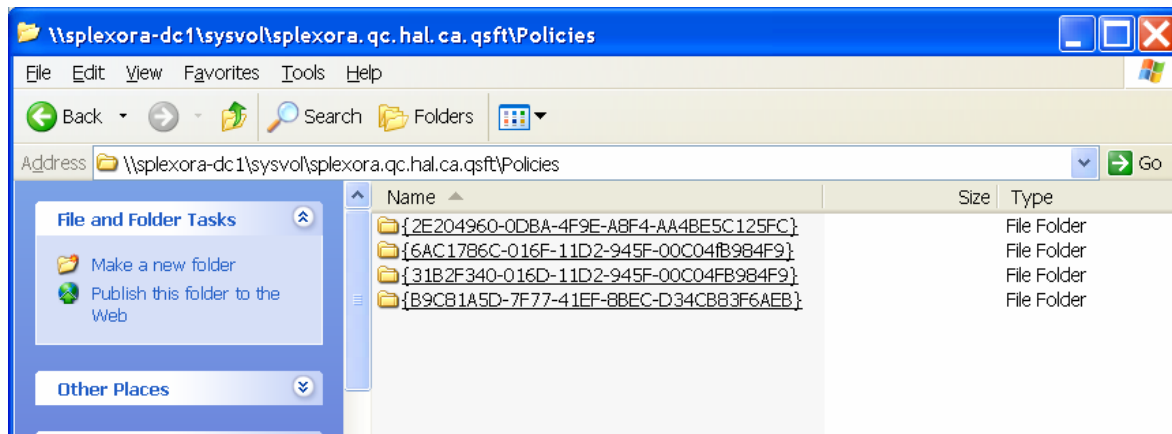


Figure 3: Viewing the contents of the GPT within a domain.

The GPT for a given GPO contains a set of folders and files that correspond to each of the areas of policy that can be set. For example, the actual settings for the Administrative Template (AT) policy within a GPO are stored in a file within the GPT called “registry.pol”. Similarly, the settings for security policy within a GPO are stored in a file called “gpttmpl.inf” in a subfolder of the GPT under \Machine\Microsoft\Windows NT\SecEdit.

The GPC and GPT typically do not require direct manipulation. The MMC Group Policy editor tools that come with Windows provide the interface to manage Group Policies without requiring interaction with these structures. However, when something goes wrong with Group Policy, knowing what is going on behind the scenes can help speed the troubleshooting process.

GPO Versioning

Because the GPO is composed of two pieces (GPC and GPT) that exist in different places (one in AD, the other in SYSVOL), there is a chance that when a GPO is modified on one domain controller, the GPC and GPT will not replicate at the same time to all other DCs within the environment. In that case, unexpected results will occur on clients processing those GPOs if the two parts are not in synch. To prevent this problem, Microsoft provides a versioning mechanism for the GPC and GPT to ensure that they are in synch as they replicate across your network. Each piece contains a version number that gets incremented when the Group Policy editor tool is used to modify a GPO. When those changes are replicated, the version numbers of the GPC and GPT must be the same on a given DC, or a client will not process that GPO.

GPO Processing

With an understanding of how GPOs are structured, let's look at how they are processed. First, Group Policy is processed only by users and computers in AD. A common misconception is that user or computer *groups* process GPOs; they do not. When a computer that is a member of an AD domain boots up, part of the boot up sequence is to process any computer-specific Group Policy that applies to that machine. When a user sits down at that computer and logs on, user-specific Group Policy that applies to that user is then processed. However, security groups can be used to *filter* the effects of GPO.

GPO Linking

When Active Directory is involved, there is a completely new set of options for deploying and leveraging Group Policy. In order to understand AD-based Group Policy, it is important to distinguish between a GPO and a link to that GPO.

Creating a new GPO from the AD Users and Computers MMC snap-in is a two-step process. It calls for first creating a new GPO (its GPC and GPT) in that AD domain, and second, linking it to the desired container object. Valid container objects include AD sites (collections of IP subnets), domains and organizational units (OUs). If a GPO is linked to an AD site, then the workstations or servers located on an IP subnet within that site will process the GPO.

Keep in mind that a site can contain machines from multiple domains within a forest. Since GPOs are stored per domain, this means that workstations or servers in domain “B” might be processing GPOs that are stored in domain “A.” This could be bad from a performance perspective because a computer or user reading the GPO must traverse trust relationships each time they process the policy.

It is possible to create a GPO that is not linked to any containers, and it is equally possible to link a single GPO to multiple containers. The default way to view and manage links is to view the Properties on a selected GPO within the AD Users and Computers MMC snap-in tool, and select the “Links” tab. Clicking “Find Now” will display all links to the GPO in the dialog (Figure 4).

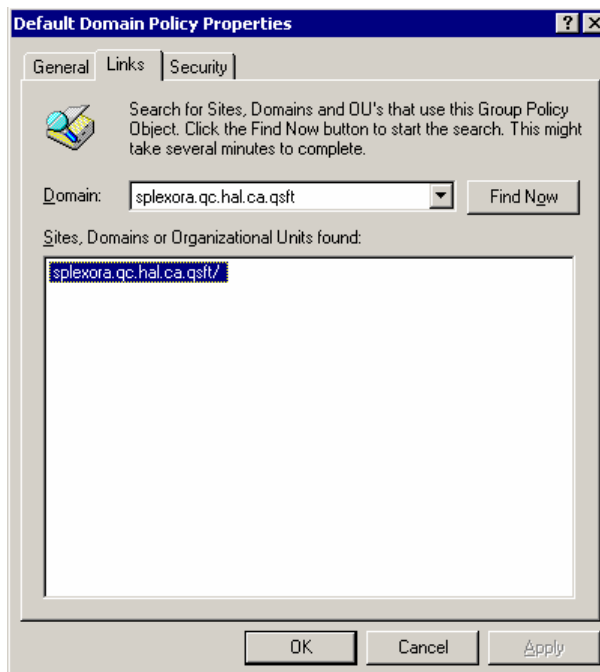


Figure 4: Displaying GPO links.

Linking a GPO to a domain allows all users and computers in that domain to process that GPO. Similarly, linking a GPO to an OU means that all users and computers residing in that OU can process the GPO. There’s nothing to prevent linking more than one GPO to any of these containers. Thus, it is conceivable to have 20 GPOs linked to a domain, 30 linked to an OU, and 30 other GPOs linked to another OU, and so on.

Obviously, life could quickly get very confusing in this scenario. When a computer boots up or a user logs on, they could end up processing many, many GPOs.

LSDOU Processing Order and Resultant Set of Policy

The accumulation of all policy settings for a particular computer or user in a particular domain, site and OU is called the Resultant Set of Policy, or RSoP (also referred to as “Group Policy Results” in Windows Server 2003).

There is an order of precedence when a computer or user processes multiple GPOs linked at many levels in an AD domain. This order, known by its acronym, LSDOU, is as follows:

- 1) The local GPO is processed first.
- 2) Any site-linked GPOs are processed next.
- 3) Domain-linked GPOs are processed next.
- 4) OU-linked GPOs are processed last.

Multiple GPOs may be linked to each container, so there is also an order of precedence for them. When viewing GPOs from within the AD Users and Computers (or AD Sites and Services for site-linked GPOs) MMC snap-in tool, you can set the order of precedence on a particular container object (Figure 5).

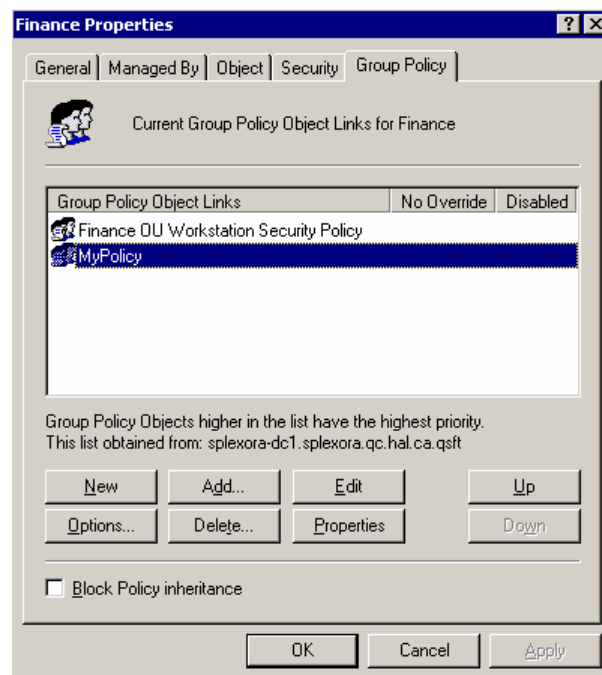


Figure 5: Viewing the order of precedence of GPOs on an OU.

You can use the Up and Down buttons to change the order of priority of the GPOs. Because GPOs at the top of the list are processed last on this container, their settings will override any conflicting settings of GPOs that are lower in the list. This override behavior also occurs when GPOs linked to different containers are processed.

A simple example would be a scenario in which there are two GPOs: one linked to the domain and one to an OU. The domain-linked GPO has a policy that removes the Run command from the user's Start Menu, but the OU-linked GPO has a policy that puts it back. Which policy would actually be applied to the computer or user? The OU-linked policy is the one the user ultimately must follow, because OU-linked GPOs are processed after domain-linked GPOs, therefore overriding the policy specified in the domain-linked GPO.

You can use the Microsoft Group Policy Management Console (GPMC) (available at <http://www.microsoft.com/downloads/details.aspx?FamilyID=0a6d4c24-8cbd-4b35-9272-dd3cbfc81887&DisplayLang=en>) to perform RSoP logging and modeling. RSoP logging allows you to see what policy was delivered to your Windows XP and Server 2003 users and computers. GPMC's RSoP logging capability will query the target machine directly and determine what policy was applied, and from which GPOs, during the last processing cycle. RSoP, which requires at least one Server 2003 DC in a forest, lets you perform "what-if" scenarios for proposed changes to your Group Policy. These "what-if" scenarios let you see what the effective policy **will** be on your users and computers prior to implementing the change.

No Override and Block Inheritance

There are circumstances, of course, where it is *not* desirable to override an "upstream" policy. A perfect example of this is security policy. A domain administrator would want to ensure that security policy that applies to an entire domain could not be overridden by a "downstream" GPO created by a local OU administrator. To prevent such a conflict, Group Policy provides for setting a No Override flag on a GPO. GPOs with this flag set will not be overridden by downstream GPOs. From the dialog box shown in Figure 5, select a GPO, choose the Options button, and set the No Override flag.

Block Inheritance does the opposite of No Override, and it can be set at the domain or OU level. A Block Inheritance setting prevents upstream GPOs from being processed altogether.

However, a GPO that has the No Override flag set will always be processed, regardless of whether an OU downstream has Block Inheritance set.

For example, let's suppose you are a domain administrator in your AD domain. You have also delegated OU administration to a number of local OU administrators, but you still need to maintain some control over their activities. Now suppose they create a GPO with Block Inheritance linked to their OU that allows their users to run the Regedit utility for viewing and editing the registry. Since this policy goes against your corporate desktop lockdown standard, you can create a GPO, linked to the domain and set to No Override, that uses AT policy to disable Regedit for all users in the domain. Because your No Override setting supersedes Block Inheritance, your OU administrators' users will no longer be able to use Regedit when next they process the policy.

Security Group Filtering

Typically, an administrator controls which computers and users will receive Group Policy, by controlling where a GPO is linked. However, there is occasionally a need for more granular control over which policies are processed by which computers and users.

For example, consider a scenario in which there is a desktop lockdown policy for a Finance OU within an AD domain. This GPO should apply to all users within the OU except for the users who have been designated OU administrators, with a lesser degree of authority than the domain administrator. In that case, how can the domain administrator control which users within the OU get the policy? The answer is to use security group filtering to control who gets which policy. To understand this, it's essential to first understand how GPO security works.

Normally, a new GPO has a set of security permissions associated with it. To view these permissions, select the Security tab from within the Properties of a GPO (Figure 6).

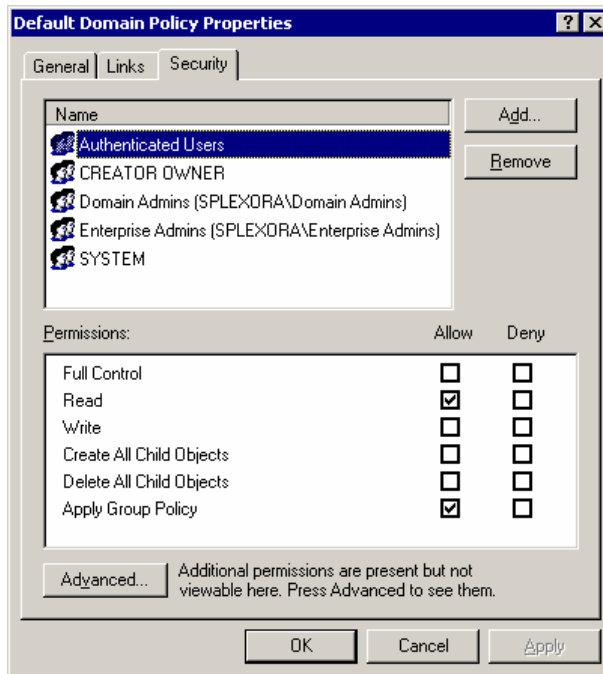


Figure 6: Viewing the security permissions on a GPO.

In Figure 6, note that the Authenticated Users group, which includes all users and computers within an AD domain, has two permissions checked: “Read” and “Apply Group Policy.” In fact, these are the only permissions a user or computer needs to process a GPO.

Authenticated Users is always granted this access by default when creating a new GPO. To target a GPO to a particular group of users or computers, this Authenticated Users Access Control Entry (ACE) must be removed and replaced with a new ACE that grants “Read” and “Apply Group Policy” permissions to the specific computer or user group that the GPO will target. Note that you could also leave the Authenticated Users ACE intact and add a Deny ACE on the group represented by the users or computers that you don’t want to process the policy.

If a GPO sets both per-computer and per-user policy, both computer and user groups can be targeted via security group filtering.

The Client's Role in Processing

We've described how GPOs are structured, where their settings are stored, and how they are linked to containers within AD. But how is the GPO actually processed at the client? How are the specified policy changes actually made? The answer lies in a set of files installed on every Windows system called Client Side Extensions (CSEs).

CSEs are DLLs that implement the actual policy processing functionality. There is typically one CSE for each kind of policy area supported in Group Policy. CSE DLLs are installed in %systemroot%\system32 when Windows 2000, XP or Server 2003 is installed. To see which CSEs are registered on a particular system, look in the registry under:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\
CurrentVersion\Winlogon\GPExtensions
```

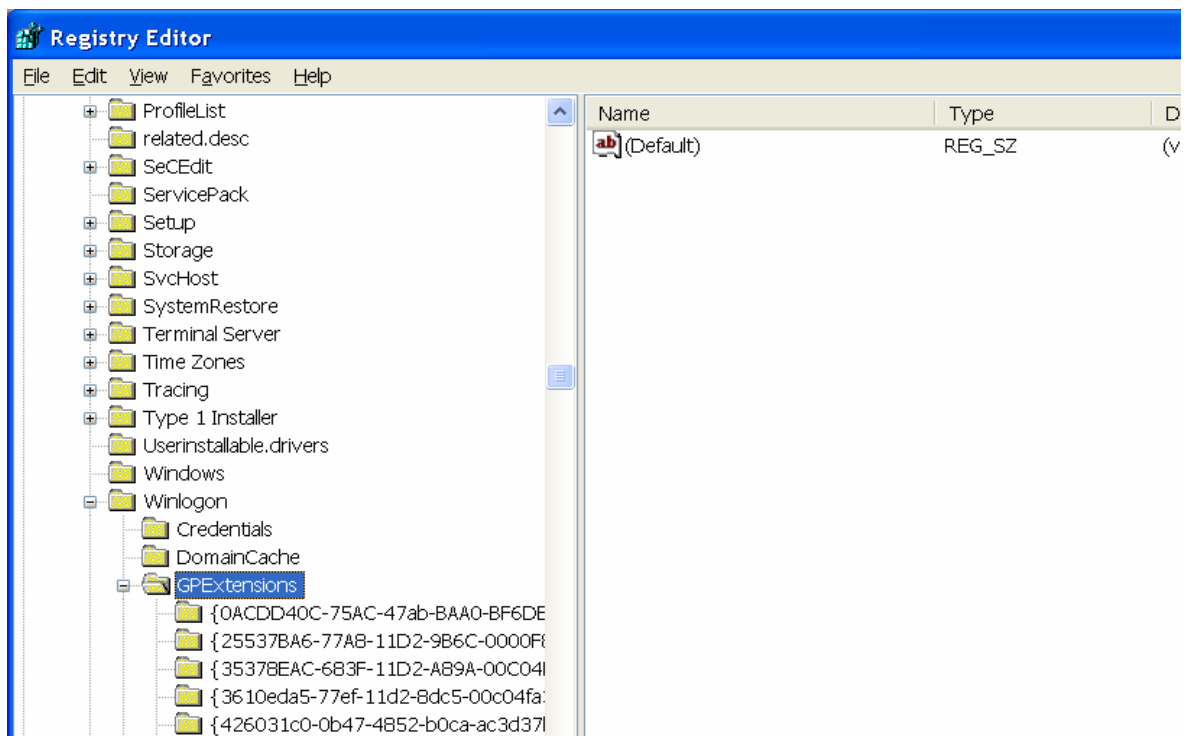


Figure 7: Registration of CSEs.

As with GPCs, each CSE is registered by its GUID. By default, any GPO whose version number does not change between processing cycles is not processed by the CSEs.

However, it is possible to override that behavior for a given CSE and process a GPO every time. For example, to enable or disable this behavior, you can set the “NoGPOListChanges” registry value within HKLM\Software\Policies\Windows\Group Policy. The registry entries that control individual CSE behaviors can be adjusted using AT policy within a GPO. Specifically, within Computer Configuration | System | Group Policy, each CSE area has a policy processing item to control how it behaves during a processing cycle.

Processing the GPOs and setting policy is done by CSEs installed on a workstation or server. But it is the Winlogon process—a privileged system process—running on that workstation or server that calls each CSE. As an example, consider the following process that occurs when machine-specific GPOs are processed at machine startup time:

- 1) As the machine boots up, it authenticates with Active Directory and determines which GPOs it must process. These are all of the GPOs linked to containers “above” the machine’s location within the AD hierarchy. The list of GPOs is built using the LSDOU precedence described above.
- 2) Once the list of GPOs that a machine must process has been created, the Winlogon process calls each CSE DLL to process that portion of each GPO it is responsible for. For example, if a workstation is getting security policy from four different GPOs, then the security CSE is called, and it processes security policy on each of those four GPOs in the LSDOU order. After security processing has completed, the next CSE is called, and it does its processing on the four GPOs.

The default behavior is for a CSE to *not* process a GPO if it has not changed since the last processing cycle. Whether a GPO has changed or not is calculated using history information that each CSE stores in the registry for each GPO it processes. Specifically, under HKEY_LOCAL_MACHINE (and HKEY_CURRENT_USER)\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\History, each CSE has a registry key that stores the last GPO version processed for each GPO that is processed. When the CSE runs the next time, it compares this registry-cached version information to the current GPO defined in AD and, if they are the same, the GPO is not processed (unless this behavior is overridden, as described above).

Background Processing

GPOs are not processed only at machine startup or user logon time. On Windows workstations and member servers, machine and user GPOs are also processed in the background every 90 minutes. Domain controllers perform background GPO processing every five minutes by default. You can change the refresh interval on both workstation/member servers and domain controllers via AT policy (Figure 8).

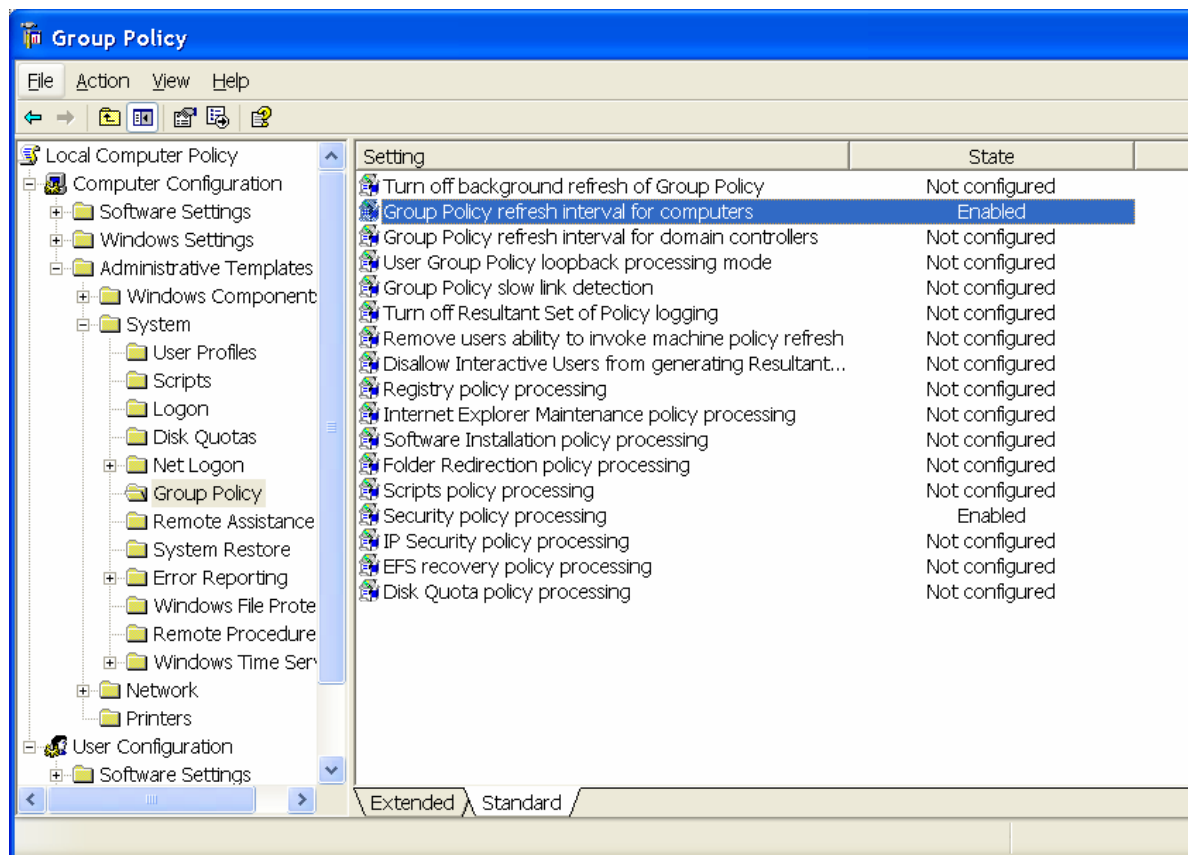


Figure 8: Modifying background refresh intervals using AT policy.

There are certain CSEs that do not perform background refresh of policy because to do so would cause unexpected results for users logged on to a workstation or server. The CSEs that don't perform this background refresh include:

- Folder Redirection
- Software Installation
- Scripts (the Scripts CSE does process GPOs on each background refresh interval, but scripts themselves don't run except at user logon/logoff and machine startup/shutdown)

To trigger on-demand processing of GPOs, use the `secedit.exe` (built in to Windows 2000) or `gpupdate.exe` (built in to XP and Server 2003) command-line utilities. When manually triggering a GPO processing update, the same rules apply in terms of not processing GPOs that have not changed or CSEs that don't normally process during background refresh.

UNDERSTANDING WHAT GROUP POLICY CAN DO

Overview of Policy Functionality

With a solid understanding of how GPOs work, let's look at how they can help you "bulletproof" your Windows infrastructure. Table 1 lists all of the policy functionality available as of Windows XP and describes what each one does. Further on, we'll explore how to take full advantage of the extensive policy capabilities in Group Policy.

Policy	Description
Software Installation	The Software Installation feature is both computer- and user-specific. This feature lets you "assign" or "publish" software applications to computers and users. Assigned applications are installed or advertised on machine startup or user logon, respectively. Published applications are per-user only and are made available for on-demand installation via the Control Panel Add/Remove Programs applet. Software Installation requires applications to be packaged using the Windows Installer (*.msi) packaging format. You can optionally install legacy-packaged setups using the .zap format, but there are limitations with this method.
Scripts	Group Policy supports machine-specific startup and shutdown scripts as well as user-specific logon and logoff scripts. Scripts can take almost any form, including batch files, Windows Script Host files, and Perl scripts. Since scripts are executed on the client processing the GPO, the client must have the required scripting environment for scripts to work.
Security	Group Policy provides the ability to extensively control a variety of security settings on Windows machines, including: Account Policy: Set password behavior Local Policy: Set user rights and advanced security restrictions Event Log Policy: Set event log size and retention policy Restricted Groups Policy: Control who can and should be a member of a user group System Services Policy: Control who has the ability to stop, start and re-configure Windows Services Registry & File System Policy: Control who has rights to certain folders, files and registry keys across machines

Policy	Description
	<p>Wireless Network Policy (XP and 2003 Server only): Control who can access wireless networks</p> <p>Public Key Policies (computer- and user-specific): Control public key certificate delivery and revocation</p> <p>Software Restriction Policies (XP and 2003 Server only, computer- and user-specific): Control which applications can run based on where those applications came from</p> <p>IP Security Policy: Control the use of IPSec on Windows networks; includes port filtering for computers implementing IPSec</p>
Administrative Template	<p>Administrative Template policy is similar to what was provided in NT4 system policy: values of specific registry keys are set on a machine- and user-specific basis. AT policies can be extended to include other registry values by creating custom *.adm template files.</p> <p>With the release of Windows XP SP2, Microsoft provided more than 600 new AT policies, including those for controlling the new Windows Firewall as well as further control over Internet Explorer security and behavior.</p>
Remote Installation Services	Remote Installation Services (RIS) policy lets administrators control the behavior of RIS servers within the environment, e.g., whether certain setup options are available as you deploy an image via RIS.
Folder Redirection	Folder Redirection policy lets portions of a user's profile be re-directed to alternate locations. By default, a user's profile is cached within the Documents and Settings folder on the user's local hard drive. Profiles can also roam with a user by specifying a server share where the profile can be stored. Folder Redirection works with both of these technologies to allow you to specify an alternate share for portions of a user's profile.
Internet Explorer Maintenance	Internet Explorer Maintenance policy can control the configuration of Internet Explorer within an environment. Use this policy to enforce everything from security zone settings to proxy settings to browser branding.

Table 1: Reviewing the policy capabilities in Group Policy.

Each of the policy areas shown in

Table 1 has unique capabilities. The following sections provide a more in-depth understanding of each policy's function.

Software Installation

The Software Installation feature within Group Policy provides an excellent departmental software distribution capability. If an administrator deploys applications to end users, Software Installation policy can supplement an existing software distribution product like Microsoft Systems Management Server (SMS).

There are two types of software installation deployments—assigned and published applications. Assigned applications can be deployed per-computer or per-user, as follows:

- When an application is assigned per-computer, that application is installed the next time the computer receiving the GPO containing the assigned application is rebooted. This is an unfortunate limitation of computer-assigned Software Installation: it can only be triggered on machine reboot. Therefore, relying on Software Installation policy is less than ideal when deploying software in environments where machines need to be available 24/7, such as in server environments. However, computer assignment may be acceptable for desktop-based deployments where reboots are more common. Note that Software Installation is a CSE that does not process policy in the background, so there is no way to manually trigger a Software Installation deployment.
- An application assigned per-user is not actually installed on the workstation when the user logs on. Instead, it is simply “advertised” to the user the first time the user calls the application or a file associated with the application. Advertisement is a feature specific to the Windows Installer (*.msi) packaging technology. When an application is advertised, it is not actually installed on the workstation; rather, it is associated with the workstation and can be installed the first time a user calls the application or a file associated with the application.

For example, when Software Installation assignment is used to advertise Microsoft Office, several things happen to the user’s workstation at logon. First, the registry is modified to associate all file extensions supported by Office with the advertised application. Second, any Start Menu or Desktop icons that are part of the Office package are installed in the user’s profile. Finally, any COM objects that have been advertised by Office are registered in the registry.

If the user opens an Office document, clicks on an Office icon, or starts an application that requires an Office-based COM object, the Windows Installer service on that workstation kicks in and installs Office. This mode of installation is called “Install on First Use.”

Applications can also be “published” via Software Installation. Publishing is supported only on a per-user basis. When an administrator publishes an application, that application appears as a choice in the Control Panel Add/Remove Programs (ARP) applet, under the “Add New Programs” section (Figure 9).

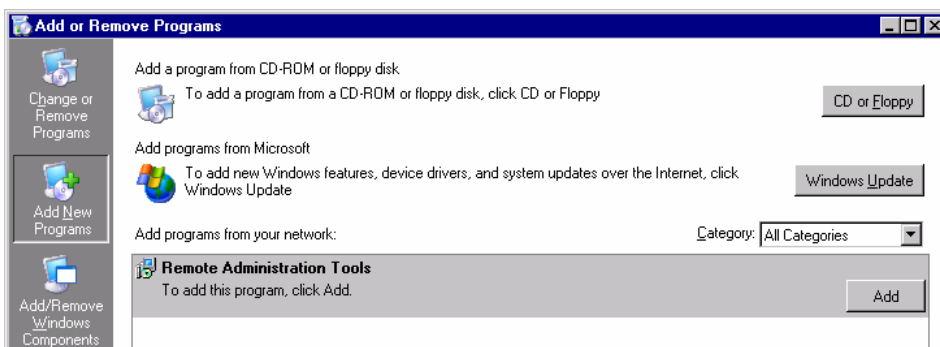


Figure 9: Viewing a published application in Add/Remove Programs.

When publishing an application, you also have the option to advertise the application if that functionality is supported within the application’s package. So even though published applications are normally only installed when the user goes into the ARP applet and selects the Add button, there are applications that can be installed on first use just like assigned applications. This gives you the best of both worlds if you have applications that you don’t necessarily want to install on every workstation automatically, but should be available for installation when the user needs them.

The final feature in Software Installation is the ability to permission individual applications. Normally, an administrator controls which computers and users process a GPO by deciding where that GPO is linked or using security group filtering (explained above). However, within Software Installation, it’s possible to set permissions on a particular deployed application to target the delivery of that application. So, with a GPO that is linked and permissioned such that all users within a particular OU will process that GPO, you can further control which deployed applications those users will receive, by modifying security permissions within that application. To modify the security on given application at deployment time, or after it has been deployed, select the Security tab on that application and grant or remove Read permission for a given user or computer group.

Scripts

Scripts policy gives Windows 2000 and XP clients more robust capabilities than the logon script capability provided with NT4. GPO-based scripts now support machine-specific startup and shutdown scripts, as well as user-specific logon and logoff scripts. Machine-based scripts run in the context of the privileged LocalSystem account. Therefore, these scripts facilitate administrative tasks that normal users don't have the privileges to execute. Similarly, logon and logoff scripts run in the context of the logged-on user, so any required user-specific tasks can be implemented in these scripts. Scripts can take almost any form, from batch files to Windows Script Host scripts to executables. In addition, there may be multiple scripts defined within a single GPO or multiple scripts across multiple GPOs. Scripts are processed one at a time, in an order that can be defined within the GPO. Scripts can be set to time out so that no one script can hang the machine startup or user logon process.

Security

The security policy settings in Group Policy form the heart of the GPO. If you implement only one feature within Group Policy, it will most likely be security policy. This is because GPO-based security policy is the only way to control domain-wide security behavior, such as password age, account lockout, and password complexity requirements. But Group Policy-based security policy offers so much more utility that it could fill another paper. The following are some of the most commonly used areas within security policy:

- **Account Policy:** Controls password behavior, intruder lockout behavior, and Kerberos lifetime behavior.
- **Local Policies:** Controls security auditing settings (which events to audit), user rights assignment (e.g., who has local logon rights), and advanced security options (e.g., disallow anonymous SAM enumeration, SMB signing behavior, etc.).
- **Event Log:** Lets you specify event log sizes and retention policy (e.g., overwrite as needed, stop writing when full).

- **Restricted Groups:** Controls group membership. Specifies who is allowed to be a member of a particular group and which groups a group must belong to. For example, only domain admins and “level 2 admins” can be a member of the local Administrators group on the domain or on individual member servers.
- **System Services:** Sets the startup state (automatic, manual or disabled) of any Windows service and sets permissions on a service to control who can stop, start, or configure it.
- **Registry & File System:** Forces security permissions on registry keys, NTFS folders and files on any GPO-linked machine.
- **Wireless Network Policy (XP and Server 2003 only):** Controls who can access particular 802.11 networks. Determines the kinds of wireless networks a computer can access (infrastructure WAP or ad-hoc peer-to-peer) and controls the preferred networks that a computer can access.
- **Public Key Policies:** Defines Encrypted File System (EFS) key recovery agents—users who are authorized to un-encrypt EFS encrypted files in addition to the file owner. Defines automatic enrollment of X.509 certificates by user or computer and provides lists of trusted certificate authorities or Certificate Revocation Lists (CRLs) for a given computer or user.
- **Software Restriction Policies (XP and Server 2003 only):** This powerful new policy feature enables restriction of what type of code (scripts, executables, etc.) can run based on four different criteria:
 - ❖ **Certificates:** Only code signed by particular certificate authorities can run.
 - ❖ **Hash:** Only code with specified hash values can run.
 - ❖ **Internet Zone:** Only code from particular Internet zones can run.
 - ❖ **Path:** Only code from specific paths can run.
- **IP Security (IPSec) Policies:** Controls network traffic between computers that are subject to the IPSec policy, which includes forcing certain computers to encrypt their network traffic using IPSec. You can also use IPSec policy to filter IP traffic to and from a computer.

Administrative Templates

Administrative Template policy is fundamental to Group Policy. Use AT policy to control registry values on a per-computer basis (within HKEY_LOCAL_MACHINE) or per-user basis (within HKEY_CURRENT_USER). AT policy is most often used to lock down user desktops to prevent user “futzing,” which can often result in expensive help desk calls. AT policy is about reducing the number of options users can get to, thereby simplifying their desktop and support of their desktop.

For example, an AT policy could remove all icons from a user’s desktop, or remove a user’s ability to launch a command shell or even to browse network resources. In short, AT policy enables very granular control over the user’s desktop experience.

AT policy can also be extended to include the setting of any registry value on a Windows system. This is done by creating custom *.adm template files that include the registry keys and desired values, and then loading them into a GPO.

Note that starting in Windows 2000, Microsoft provides a mechanism that prevents the “tattooing” of the registry when AT policy is no longer applied to a user or computer. That is, in NT4, when a system policy file was removed from a domain, the registry entries that it specified remained on the machine and had to be explicitly removed by a new policy that reset those values. In Windows 2000, XP, and Server 2003, that is no longer the case for all registry entries. Any AT policies that set registry values under the following keys will be removed when the policy no longer applies:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies  
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies  
HKEY_CURRENT_USER\SOFTWARE\Policies  
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies
```

AT policy settings made under any of these keys are known as “policies” and do not suffer the fate of “tattooing.” If you create any AT policies that make changes to other areas of the registry, these are referred to as “preferences” and will be “tattooed” into the registry until they are explicitly removed.

Remote Installation Services Policy

The RIS policy within Group Policy applies to users who are installing computers into an AD domain using an RIS server. Options within this policy enable control of the options that the user has when the RIS installation begins. For example, you can set policy that hides the Tools option that RIS displays as part of its menu of choices when you begin an RIS-based installation.

Folder Redirection

Folder Redirection policy lets you control portions of the user's profile, redirecting it to alternate locations such as server shares. Folder Redirection supports redirection of the following four folders within a user profile:

- Application Data
- Desktop
- My Documents (and My Pictures)
- Start Menu

Folder Redirection supports two different types of redirection: basic and advanced. Basic redirection redirects all users subject to the policy to a specific location. For example, a company may want to redirect all users' My Documents folders to their respective home folders on a server share. In this case, an administrator might specify `\\server\home\%username%\My Documents` as the path.

Advanced redirection goes one step further by specifying a different redirection path based on the user's group membership. For example, you might specify one server share for members of the Accounting user group and another for members of the Marketing user group. Folder Redirection policy can also control the look and feel of the user's desktop. An example is to redirect users' desktop folders to a read-only server share that specifies a fixed number of icons that they have access to.

Folder Redirection can work in conjunction with the Offline Folders feature of Windows. For example, if the My Documents folder within a profile has been cached for offline use and it has been redirected to a server share, then the My Documents folder will always be available, even if the user is not connected to the network.

Internet Explorer Maintenance

Internet Explorer Maintenance policy enables control of the configuration of the Internet Explorer settings of end users. IE Maintenance policy includes the following policy settings:

- **Browser User Interface:** Controls the look and feel of IE, including the browser window's title and any custom bitmaps and custom toolbars
- **Connection:** Includes connection settings (e.g., LAN and dial-up settings), automatic proxy behavior, proxy server settings, and custom user agent strings
- **URLs:** Specifies a pre-set list of Favorites or important URLs
- **Security:** Sets Internet Zone security, Content Rating settings and Authenticode settings
- **Programs:** Specifies the default programs that IE lets you control, such as that Outlook Express is the default e-mail client or that FrontPage is the default HTML editor

IE Maintenance policy enables two modes for policy application: mandatory and preference modes. Mandatory mode enforces IE settings each time the GPO is applied to a user. Preference mode sets IE settings once and then gives the user the ability to change them after the policy is applied. These two modes offer some flexibility for those users who must have standard settings and those users who need some standard settings but also need the flexibility to modify them over time.

IE Maintenance policy can come in handy when you need to centrally manage a user's Web browsing experience. For example, you could use this policy to reduce help desk calls from users wondering what their HTTP proxy settings should be. Or, you can use this policy to distribute links or Favorites to frequently-used internal corporate sites, or even links to specific events that will be displayed on the Web, such as executive presentations.

DESIGNING A BULLETPROOF GROUP POLICY IMPLEMENTATION

The complexity of Group Policy and all of its available policy options tends to discourage enterprises from taking full advantage of this powerful technology. Compound this with the fact that there are very few native tools for really making sense of Group Policy, and the result is a technology that is sorely under-utilized.

However, by taking time to learn about Group Policy, and with the support of Group Policy management tools like Group Policy Manager provided by Quest Software, you can really bulletproof your network while delivering on the promise of a highly managed, cost effective computing environment. This section presents an approach to GPO implementation that reduces the out-of-the-box complexity to something much more manageable.

When most organizations are designing their GPO implementations, the first step they typically take is to utilize only the bare minimum of GPO functionality in order to get up to speed and get comfortable with how Group Policy works. For example, Group Policy must be utilized to set domain-wide security account policy. But why stop there? Group Policy is capable of much more. The first step is to take Group Policy into consideration when designing an AD namespace.

Active Directory Namespace Planning and Group Policy

Many Windows engineers make the mistake of planning their AD namespace without considering how Group Policy may fit in down the line. This usually results in a less-than-optimal GPO implementation. The key to effectively designing an AD namespace with Group Policy in mind is based on understanding the different options for deploying Group Policy. Think of the GPO design problem in two ways:

- Where do I link my GPOs?
- How monolithic should my GPOs be?

Where Do I Link My GPOs?

GPOs can be linked at the site, domain, or OU levels within an AD domain. Any users and computers that are located “downstream” from a GPO will process that GPO. The primary exception to this “downstream” rule is using security group filtering to specify which computer and/or user gets which GPOs. The problem with security group filtering is that it can become complex and therefore prone to error. Over time, more and more security groups may need to be added to a GPO to control exactly which computers and users process the GPO.

For this reason, a rule of thumb is to always link a GPO as “close” to its intended target as possible. For example, to lock down the desktops of users in one or more OUs, it may be tempting to link a GPO at the domain level to cover all of the OUs required, and then use security group filtering to control which users actually get the policy (**Figure 10**).

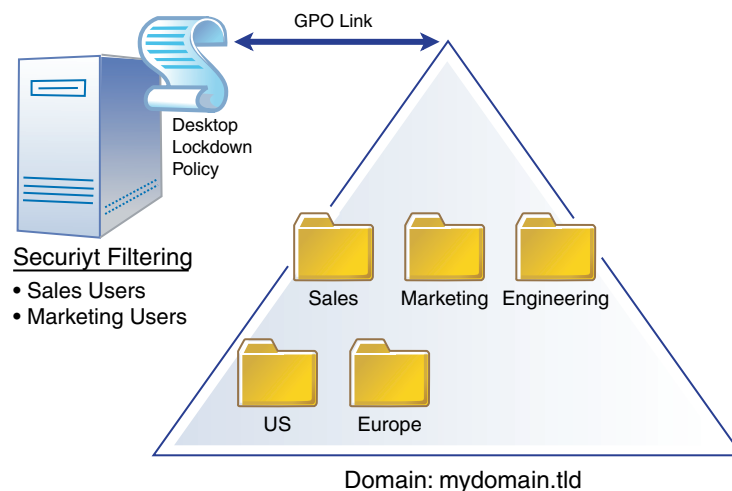


Figure 10: Viewing a GPO linked to the domain.

As **Figure 10** shows, a GPO is linked to the domain where it will apply to all users in Sales and Marketing OUs via security group filtering. This mechanism works fine in the short term, but over time, if you want to include more users across different OUs, then the list of security filters will grow. Additionally, if there are other GPOs that you need to link to those OUs, then you will have to contend with a complex set of permutations to determine which GPO settings will apply to users when they log on.

Another consideration for GPO linking is your administrative delegation model. Active Directory lets you delegate the ability to link and un-link a GPO from a container object. If you want to grant this permission to your OU administrators to give them control over which GPOs they process for their OU, then linking all of your GPOs to the domain level will not help their cause.

The best practice is to always link a GPO as close to its intended target as possible. It's okay to link a GPO to a domain knowing that, with few exceptions, all computers and users in that domain will need to process that GPO. But if the GPO may change over time or if there's another GPO that provides more granular settings to certain groups of users or computers, then it is wisest to link the GPO to each OU where those users and computers reside. Figure 11 shows what would happen if we took this approach instead of that shown in Figure 10.

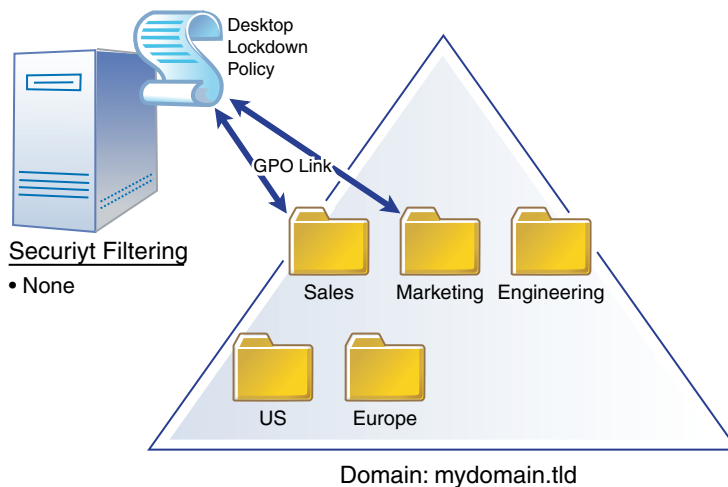


Figure 11: Linking a GPO to associated OUs instead of to the domain.

In Figure 11, the original Desktop Lockdown policy is now linked directly to the Sales and Marketing OUs and no longer depends on security group filtering to control who receives the policy. The following bullets summarize the best practices for where to link a GPO:

- If the GPO contains policy that will be processed by the entire domain with few exceptions, then link the GPO at the domain level.
- If the GPO contains policy that is specific to one or more OUs, then link that GPO to those OUs. If each OU requires some unique policy settings that are different from another OU, then create individual GPOs that apply to each OU.
- If policy must be applied based on a computer's location on an IP network (i.e., its subnet), then use site-linked GPOs.

How Monolithic Should My GPOs Be?

Since a single GPO contains many different policy settings from security to software installation, it's certainly possible to create a few monolithic GPOs in a domain to set all of its policy. Unfortunately, that is not necessarily the most manageable approach. Many enterprises are finding it better to use functionally focused GPOs—GPOs designed to serve a particular purpose. For example, instead of have a single GPO that provides IE Maintenance, workstation/member server security, and desktop lockdown, a company might design three separate GPOs that provide these three functions. That is, policy is “layered” onto a particular target set of users and computers rather than being provided in one or two more complex GPOs. The advantages and challenges of this functional approach as compared to the monolithic approach are shown in Table 2.

Metric	Advantages of functional GPOs	Disadvantages of functional GPOs
Ease of Administration	<p>Easier to delegate. For example, you can easily have one group of administrators specifying security policy, and another specifying lockdown policy. There is no easy way to do this if both types of policy are specified in a single GPO.</p> <p>Less chance of errors causing a cascading effect across other policy areas.</p>	<p>More GPOs to manage.</p> <p>More places to look for policy settings.</p>
Flexibility of Policy Settings	<p>Much more flexible.</p> <p>Easier to test before deployment: a single policy change affects only the GPO that contains that change.</p> <p>Easier to re-use GPOs.</p>	<p>None.</p>
Processing Performance	<p>None.</p>	<p>Having more GPOs can decrease performance. However, GPOs that do not change from processing cycle to cycle are not processed, so if the majority of your functional GPOs do not change frequently, there should be no major performance impact.</p>
Calculating RSoP and Troubleshooting	<p>Easier to troubleshoot problems: since policies are divided into functional GPOs, it's easier to pinpoint where a setting is coming from.</p>	<p>Calculating RSoP can be more difficult because it involves the overlay of more GPOs.</p>

Table 2: Advantages and disadvantages of functional GPOs.

The choice of approach in a GPO implementation will likely be driven by your individual needs. For example, if your primary need is to be able to delegate individual policy areas to different administrators, then the functional approach is the way to go. If you have only one or two administrators managing Group Policy, then the monolithic approach will prove simpler. And, in some cases, a combination of the two approaches is the right way to go.

Now let's look at some best practices for setting policy in some of the major policy areas.

Best Practices for Security Policy

The security policy options are perhaps the most used feature within Group Policy. They provide the most obvious advantages in terms of securing large numbers of Windows devices consistently. However, there are definitely some hazards to be aware of when deploying security policy. Keep the following items in mind when designing your security policy implementation:

- **Domain-wide account policy** can be deployed only from a GPO linked to the domain. For example, to require users to use eight-character passwords when they log on to a domain, this policy must be set in a GPO linked to the domain. The domain-linked GPO is the only place where domain-wide account policy can be set. It can't be done in a GPO linked to an OU, not even the domain controller's OU. The best implementation practice is to create a separate GPO that sets only domain-wide account policy, and to set this GPO to No Override to prevent other domain-linked GPOs from overriding it. Then, permission that GPO such that only a select few number of administrators or security officers can edit it.
- **Member server/workstation account policy.** If you want to set different account policy for local accounts found on workstations and member servers, you *can* do so using GPOs linked to OUs.
- **Other domain-wide security policy** such as user rights assignment, auditing, event log configurations on domain controllers, advanced security options, etc. must be set on a GPO linked to the domain controller's OU. Such policy will be ignored if, for example, you set it on a GPO linked at the domain level. Note that this holds true for domain-wide settings only—that is, settings that apply to users and computers authenticating to the domain, rather than to a local computer.
- **Security templates** can be used to build *standardized security configurations* that can then be applied to GPOs. Microsoft provides a number of standard security templates in the %systemroot%\security\templates folder. You can also create custom security templates for your environment using the MMC Security Templates snap-in. Security templates are a good way to manage standard security policy outside of live production GPOs. Managing templates instead of the actual GPO will ensure that there is always a known good copy of what security policy *should* be, and the template can be re-applied to production GPOs if needed.

Best Practices for AT Policy

Administrative Template policy is probably the next most frequently used area within Group Policy. The use of AT policy is pretty straightforward, but here are some tips for maximizing its value:

- **Be aware of the difference between preferences and policies.** As mentioned earlier, policies will not tattoo the registry, but preferences will. By default, when editing a GPO, the preferences that Microsoft includes in the base *.adm files are not visible. To view any preferences that may be defined, highlight the Administrative Templates node within the Group Policy MMC snap-in, select the View menu, and clear the “Show Policies Only” option. Preferences are distinguished by a red-colored icon next to the setting (Figure 12).

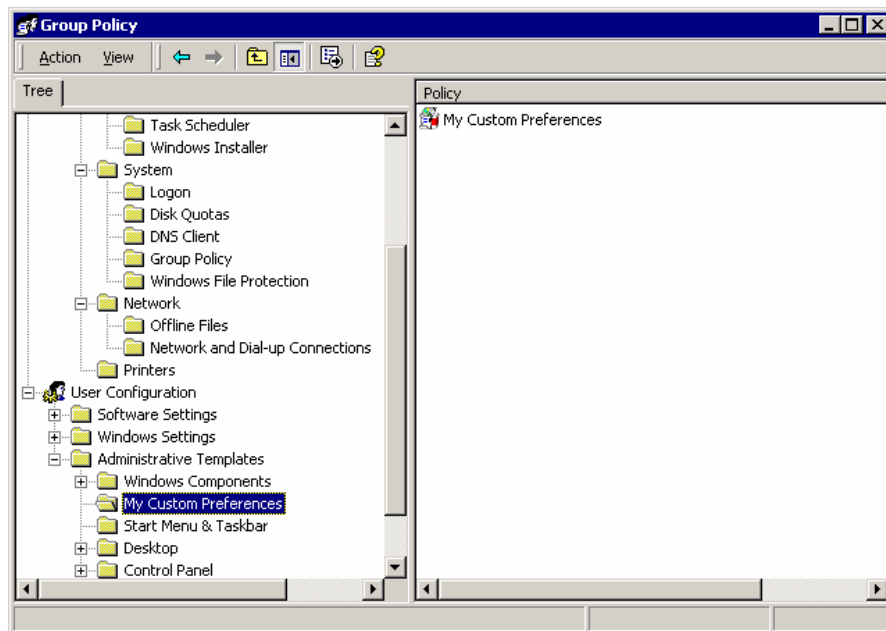


Figure 12: Viewing a preference within the Group Policy MMC snap-in.

- **When creating a custom *.adm file** you have to add it to the GPO in order to see it. To add a custom *.adm file to a GPO, simply right-click the Administrative Templates node on either Computer Configuration or User Configuration within the Group Policy editor tool and select “Add/Remove Templates.” After you add the template file, the *.adm file is actually copied to the ADM folder within the GPT stored on SYSVOL. Thus, to use an *.adm file on another GPO, repeat this copy process on that GPO.

- **AT policy has three states: enabled, disabled, and not configured.** A policy that is enabled can mean different things, depending on how the policy is written. If you have two GPOs, one setting policy item A to “enabled” and the other setting policy item A to “disabled,” then the downstream GPO will ultimately decide what policy item A is set to. Note that if one GPO has policy item A set to “disabled” and the other GPO has it set to “not configured,” then the policy will be set to “disabled” regardless of the processing order of the GPOs.

Best Practices for Other Areas of Group Policy

Here are some other tips for the other areas of Group Policy:

- When using **IE Maintenance** policy, keep in mind that there are two modes—mandatory mode and preference mode. Before switching from preference mode to mandatory mode, all of the browser settings within the GPO will need to be reset. If some users need mandatory settings and some need preference settings, the best practice is to create two GPOs and then use security group filtering to apply the appropriate GPO to each of the user groups (if the users all reside in a single OU).
- When using **Folder Redirection** policy to redirect folders like My Documents, make sure you check the settings option in the GPO that says “Grant the User Exclusive Rights to My Documents.” This changes the NTFS permissions on the folder where you’ve redirected My Documents, to allow only the user’s account (and the LocalSystem account) access to the folder. This ensures privacy of the user’s data. If you don’t check this option, the permissions on the folder created by redirection will simply be inherited from the parent folder. Also, don’t redirect a folder to a Distribute File System (DFS) share if it contains read-write data and your DFS shares are replicated. This will cause file synchronization issues.
- Understand the limitations of **Software Installation** policy before implementing it. You can do an unattended installation of software only if you assign an application to a machine—and even then you need to re-boot that machine for the software installation to occur. Also, keep in mind that if you are using .zap files (legacy setups rather than .msi), you can only publish the application, and when the users install it, they don’t get the benefits of privilege escalation that .msi-deployed apps do. This means that users must have sufficient privileges on their workstation to install the application. Software Installation policy is really best for doing small departmental deployment jobs. It does not take the place of an enterprise software distribution tool.

CONCLUSION

Group Policy is both powerful and complex. Powerful, in that it provides a myriad of ways to secure and manage Windows resources. Complex, because the native tools leave it up to you to do the heavy lifting of getting the most from this technology. To take full advantage of Group Policy requires proper knowledge of best practices to ensure consistent, expected application of policy.

ABOUT THE AUTHOR

Darren Mar-Elia, Chief Technology Officer for Windows Management at Quest Software, has more than 15 years of experience in systems and network administration, design and architecture, with a focus on and expertise in large-scale enterprise implementations of Windows infrastructures. Prior to joining Quest Software, Mar-Elia was the director of Windows architecture and planning for Charles Schwab & Co., Inc. In that capacity, he was technical lead for the company's Windows NT and 2000 design and migration efforts. He frequently speaks at conferences on Windows infrastructure topics and has been a contributing editor for Windows & .NET magazine since 1997. Mar-Elia has also written and contributed to ten books on Windows NT and 2000 and was recently awarded Microsoft MVP status for his work in the Windows Server Management community. He has a B.A. degree in organizational behavior from the University of California, Berkeley.

ABOUT QUEST WINDOWS MANAGEMENT

Quest Software, now including the people and products of Aelita Software, provides solutions that simplify, automate and secure Active Directory, Exchange and Windows environments. The Quest Windows Management group delivers comprehensive capabilities for secure Windows management and migration. For Group Policy management, Quest offers Group Policy Manager. Group Policy Manager is built on top of the Microsoft Group Policy Management Console (GPMC) to augment native functionality with offline GPO editing, enhanced RSoP reporting, archival and restoration, version control, change notification and approval, and quick rollback in the event that a GPO change has unexpected results.

For more information on Quest Software's Windows Management group, please visit <http://www.quest.com/microsoft>.

ABOUT QUEST SOFTWARE, INC.

Quest Software, Inc. provides business-critical software for 18,000 customers worldwide, including 75 percent of the Fortune 500. Quest offers products for application performance management for packaged applications and Java environments; database management for Oracle, DB2, SQL Server, Sybase and MySQL environments; and Windows management in Active Directory and Exchange. These management solutions help customers develop, deploy, manage and maintain the IT enterprise without expensive downtime or business interruption. Headquartered in Irvine, Calif., Quest Software can be found in offices around the globe and at www.quest.com.

Quest Software
Windows Management

6500 Emerald Parkway
Suite 400
Columbus, OH 43016
USA

Phone: 614-336-9223
1-800-263-0036

NOTES