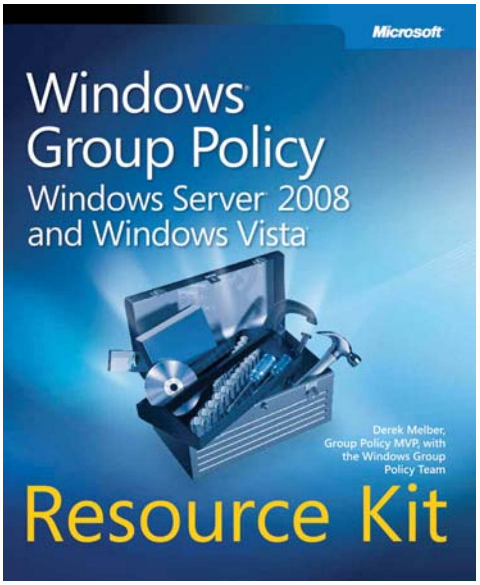


# Windows® Group Policy Resource Kit: Windows Server® 2008 and Windows Vista®

*Derek Melber, Group Policy MVP, with the Windows Group Policy Team*

**PREVIEW CONTENT** This excerpt contains uncorrected manuscript from an upcoming Microsoft Press title, for early preview, and is subject to change prior to release. This excerpt is from *Windows® Group Policy Resource Kit: Windows Server® 2008 and Windows Vista®* from Microsoft Press (ISBN 978-0-7356-2514-3, copyright 2008 Derek Melber (Content), all rights reserved), and is provided without any express, statutory, or implied warranties

To learn more about this book, visit Microsoft Learning at
http://www.microsoft.com/MSPress/books/9556.aspx

978-0-7356-2514-3

# Table of Contents

## Chapter 2

# What's New in Windows Vista and Windows Server 2008 with Group Policy

There has been a distinct push to make Group Policy a more integrated, reliable, stable, and useful product within Active Directory. That is not to say that it has not been all of these things. It is to say that efforts within the Group Policy team and the supporting teams that tie into Group Policy have put great effort into making Group Policy everything and more.

Each iteration of Group Policy has brought something grandeous. The continual improvement of technology is a testament to the different teams working on making technology work better and more efficiently for customers.

## Remember When

If you look back at some of the major milestones in the life and times of Group Policy, you will see that there have been distinct times when some radical and amazing changes came. Table 2-1 summarizes these milestones.

**Table 2-1 Group Policy Technology Milestones**

| Place in Time | Feature |
|---|---|
| Windows 2000 | Approximately 900 Total Group Policy settings |
| Windows XP | Approximately 1400 Total Group Policy settings |
| Windows Server 2003 | Group Policy Management Console introduced |
| Windows XP SP2 | Approximately 1600 Total Group Policy settings |

Of course, Windows 2000 introduced Group Policy and ended up with about 900 settings before Windows XP shipped. When Windows XP shipped, there was a bit of “flux” in the industry, as administrators tried to juggle the Windows 2000 settings, Windows XP settings, and ADM templates that shipped with each operating system. The Group Policy Management Console was a major improvement, as it moved the administration of GPOs from the Active Directory Users and Computers snap-in to the GPMC snap-in. Of course, the GPMC also gave a lot of new functionality, which we will discuss in Chapter 7, “Using the GPMC.”

When Windows XP Service Pack 2 arrived, it was a milestone not only for Group Policy, but for Microsoft as a company. The security efforts that came along with SP2 are revolutionary and what Microsoft often uses as a baseline for any desktop operating system. In many ways, Microsoft views the WindowsSever 2003 partner to Windows XP SP2, which is Service Pack 1, as the baseline for server operating systems.

# New and Now

Now that Windows Vista and Windows Server 2008 have arrived, so have some new and cool technologies for Group Policy. Don't fret. The same great features are still there; they have just been enhanced and made more spectacular. Settings have expanded, new features are abound, and many "features" that the community have wanted for a long time have finally arrived.

There are some features that came with Windows Vista. Since Windows Vista was released quite a few months before Windows Server 2008, some of these technologies might be more familiar to you. With Windows Server 2008, there were some great new features tied into the GPMC which will make administrative life much simpler when working with Group Policy. Still other technologies are outside of both Windows Vista and Windows Server 2008 at this time. They are the products that were acquired from DesktopStandard, including Advanced Group Policy Management and PolicyMaker technology.

## New Group Policy Features in Windows Vista

It has been about a year since Windows Vista arrived on the market. The new features that it brought are making big waves in the Group Policy community. It is nice to write about technology that is proven, instead of technology that is still yet unknown in the overall marketplace.

Windows Vista not only provides some very cool new graphical enhancements, but it comes with some overall changes to Group Policy that can affect the entire network of desktops— not just single machines. However, there is one change that does affect just one desktop at a time, which is the Multiple Local GPO enhancements. The other new features can affect one desktop or many desktops. Those include:

- Network Location Awareness
- ADMX Templates
- ADMX Repository
- Improved Logging

### Multiple Local GPOs

First, you need to get your bearings to understand what has changed with local GPOs on a Vista desktop. In previous versions of Windows there was a single local GPO, then there could be many GPOs in Active Directory linked to the domain, organizational units, and sites. The local GPO had no power over the Active Directory GPOs, unless there were non-conflicting settings established. In this case, the local GPO settings would make its way through the maze of Active Directory GPOs to the Resultant Set of Policies that molded the final policy settings on the computer.

Multiple local GPOs were put into place to solve many issues. One of the biggest problems this feature solves involves both users and administrators logging on to the same desktop. Until now, if there are local GPOs constraining the user account, both the administrator accounts and regular user accounts will receive the settings. This causes some very odd results, either allowing the user to have too many privileges or restricting the administrator too severely. If the administrator needs to run elevated tasks in a restricted environment like this, he or she is forced to use "Run As" or other privilege-elevating technologies. Although this is an almost ideal situation, it can cause some issues with a company that does not want these restrictions on administrators logging into desktops.

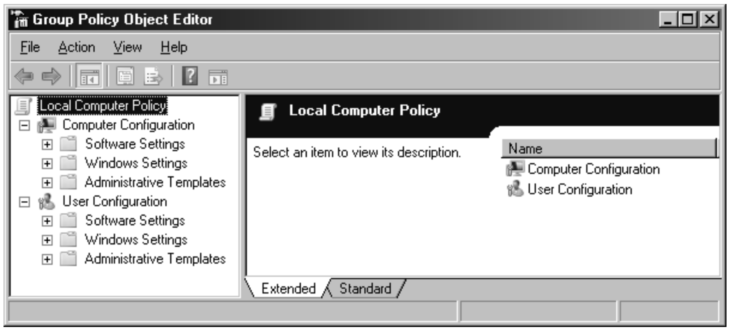
WindowsVista tackles all of these issues with new technology surrounding the local GPO. In reality, there is no longer just a single GPO on the local desktop, but three local GPOs. These three GPOs provide granular control over the different users that log on to the desktop. Local GPOs can be used in a single computer environment, home environment, small business environment, or even large corporate scenario.

The three local GPOs are designed to control different users that log on to the desktop and to be hierarchical. This hierarchy allows control over the settings that will be configured in GPO. The GPO options consist of the following:

- Local Policy Object
- Administrators and Non-Administrators Local GPOs
- Specific User Local GPO

### Local Policy Object

The Local Policy Object is identical to the local GPO that you know and love in Windows 2000 and Windows XP. It can be accessed using the Group Policy Object Editor (running Gpedit.msc from the Start, Run menu) or using the Microsoft Management Console (MMC). In either case, you are able to configure both Computer Configuration and User Configuration settings. This can be seen in Figure 2-1.



Select an item to view its description.

**Figure 2-1** The Local Group Policy can be opened in the Group Policy Object Editor by clicking Start, Run and the typing gpedit.msc in the Run dialog box.

### Administrators and Non-Administrators Local GPOs

The Administrators local GPO and non-Administrators local GPO are new in Windows Vista. As the name indicates, these GPOs are designed to control two types of user accounts. The delineation is based on which users have membership in the local Administrators group.

> NoteUser accounts having membership in the Power Users group are not considered Administrators and won't be affected by GPO settings under the Administrators local GPO. Rather, they will be affected by the GPO settings in the non-Administrators local GPO.

The reason for this delineation is quite obvious. The settings for administrator type accounts and non-administrator type accounts should be different on a desktop. Without these two options for local GPOs, it is nearly impossible to make a separation between these two types of user accounts.

These two GPOs are not as easy to access however. To access these GPOs, you must use the MMC. This exposes both of these GPOs for you to administer them, as shown in Figure 2-2.

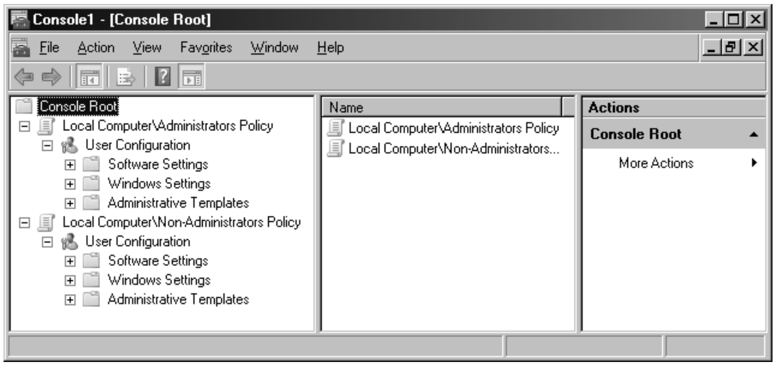


**Figure 2-2** Both the Administrators local GPO and non-Administrators local GPO can be edited in the MMC.

## Specific-User Local GPO

The final local GPO that you have at your disposal is the user-specific local GPO. This GPO offers the ultimate in granular control because it allows you to specify an individual user account to receive special GPO settings. This GPO option should not be used very often because individual user account settings are typically discouraged from an administrative efficiency standpoint.

Where this type of GPO is very useful is on specialized desktops throughout the environment. This desktops might include those functioning as a kiosk, those in a training or educational facility, or even those that have a shared user account. In these cases, the user account that is used to logon to these special desktops has a unique set of GPO settings, where all other user accounts are controlled by the Local Policy Object or even one of the Administrators local GPOs.

The administration of this GPO is also not accessed through the Group Policy Object Editor directly, rather, it is accessed through the MMC. When using the MMC to open up this GPO, you will be able to select the GPO that is associated with any one of the local user accounts that are configured in the local Security Accounts Manager (SAM). Once you add your GPO into the MMC, the interface that you will see only includes User Configuration settings. Since this local GPO only affects user accounts, the Computer Configuration settings have been removed so that they do not confuse the administrator of the local GPO. This can be seen in Figure 2-3.

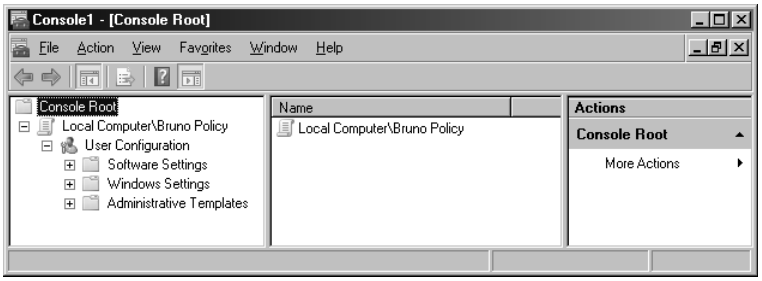


**Figure 2-3** The local user-sSpecific GPOs  can be edited in the MMC and only give the ability to control User Configuration settings.

### Precedence and Application

Now that there are multiple local GPOs to configure and choose from, it is important to understand how they are tiered in the hierarchy, in case there are ever any conflicting settings between them. The hierarchy of local GPOs creates the precedence in which they will be structured for conflicting settings. The local GPOs have a precedence; the more generic GPO has little precedence and the most specific GPO has the most precedence. Thus, the local Group Policy object has the least precedence, the user-specific local GPO has the highest precedence, and the Administrators local GPOs fall in between these two.

The precedence of the local GPOs also must play along with the GPOs that are linked within Active Directory. The same rules here apply as they did before, where the local GPOs have the weakest precedence when being compared to the GPOs from Active Directory.

## Network Location Awareness

The Microsoft Windows Network Location Awareness technology that was delivered in Windows XP has been a successful solution for many aspects of the operating system and network connectivity. This technology allows for the computer to be fully aware of its state and communication capabilities, thus allowing it to make intelligent decisions based on that state.

Group Policy has historically relied on reliable, yet not the most impressive, network identification technology available. In the past, Group Policy has used the Internet Control Message Protocol (ICMP) to determine the state of the network, as well as for network link speed. ICMP, which impompasses the PING command, is great for getting some network information, but has not been ideal for helping Group Policy application.

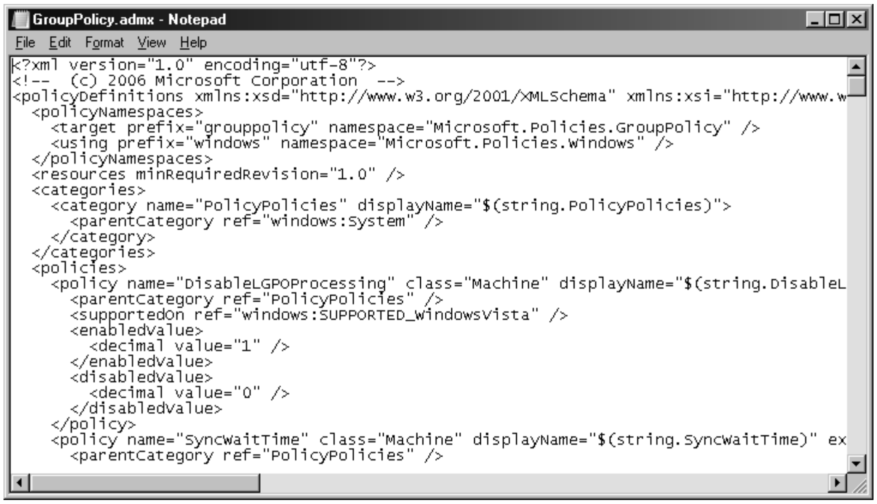
Now that Group Policy relies on network location awareness, the overall picture and state of Group Policy has been enhanced. Group Policy uses network location awareness in two primary fashions. First, it uses it to determine link speed. Second, it uses network location awareness to determine wheter the computer needing to refresh Group Policy is connected to the domain.

For this first use of Network Location Awareness, Group Policy determines if the link from the computer receiving GPO settings has a fast or slow connection to the domain and domain controllers. Since some GPO settings can take a long time to apply due to the amount of data that is being sent, determining link speed can be an indicator as to whether the data should be sent at all. Network Location Awareness provides this by determining the bandwidth of a TPC connection. This information can then be used by Group Policy to make decisions as to what settings will be delivered based solely on the bandwidth (slow link speed) that is available.

Group Policy also uses Network Location Awareness for background refreshes. This is accomplished by Network Location Awareness indicating whether the computer authenticated to a domain controller and whether the domain controller is available to the computer. This is important for computers that have failed to refresh Group Policy because the domain controller was not available. In the past when Group Policy failed to apply, the computer would wait until the next refresh interval—90 to 120 minutes—to attempt to apply Group Policy. The domain controller might have been available only minutes after the failed refresh, but the system would still wait the full refresh interval to apply the Group Policy updates. With Network Location Awareness, the computer does not wait the full refresh interval. Instead, as soon as the connection to the domain controller is detected, the Group Policy refresh occurs.

## ADMX Templates

A change that surprised some, but was needed, was a new form of Administrative template. The old ADM formatting was limiting in many ways, so a new format was developed. The new format, based on XML, has more flexibility and power than the old-style format. The new XML-based files have an ADMX extension and have changed substantially from their predecessors. A sample of the new XML formatting can be seen in Figure 2-4.



```
<?xml version="1.0" encoding="utf-8"?>
<!--  (c) 2006 Microsoft Corporation  -->
<policyDefinitions xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w
  <policyNamespaces>
    <target prefix="grouppolicy" namespace="Microsoft.Policies.GroupPolicy" />
    <using prefix="windows" namespace="Microsoft.Policies.Windows" />
  </policyNamespaces>
  <resources minRequiredRevision="1.0" />
  <categories>
    <category name="PolicyPolicies" displayName="$(string.PolicyPolicies)">
      <parentCategory ref="windows:System" />
    </category>
  </categories>
  <policies>
    <policy name="DisableLGPOProcessing" class="Machine" displayName="$(string.DisableL
      <parentCategory ref="PolicyPolicies" />
      <supportedOn ref="windows:SUPPORTED_WindowsVista" />
      <enabledValue>
        <decimal value="1" />
      </enabledValue>
      <disabledValue>
        <decimal value="0" />
      </disabledValue>
    </policy>
    <policy name="SyncWaitTime" class="Machine" displayName="$(string.SyncWaitTime)" ex
      <parentCategory ref="PolicyPolicies" />
```

**Figure 2-4** The ADMX files now are based on XML for flexibility of languages and ease of administration.

The new XLM formatting was adpoted primarily for its language flexibility. The earlier ADM formatting did not translate into other languages, forcing other countries and languages to use English, which is not always feasible. During the migration to the new format, the structure of the ADM files was radically enhanced too. With the ADM structure, all settings lived in five ADM files. Now, there are 132ADMX files that contain all of the administrative template policy settings. Figure 2-5 shows some of thes policy settings.

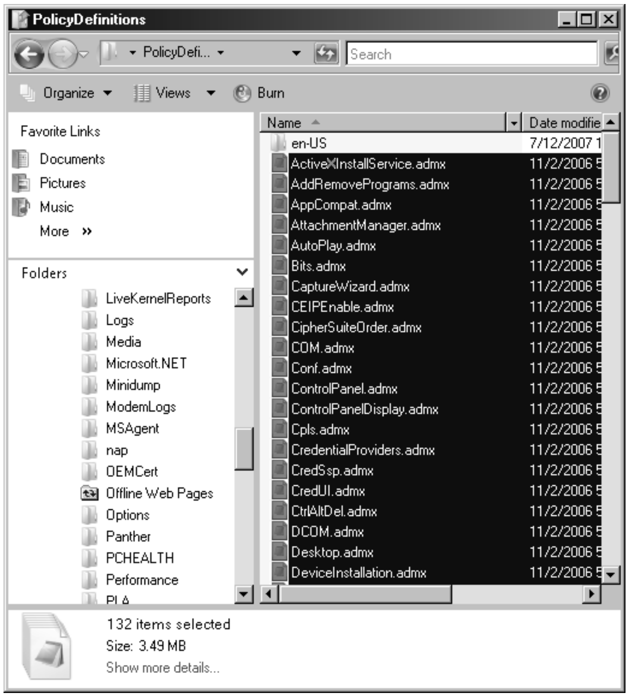


**Figure 2-5** Now that the ADMX files are XML-based, there are 132 individual templates that make up the Administratative Templates section of a GPO.

> NoteADMX files, their structure, and details are described in detail in Chapter 10, "Customizing Administrative Templates."

These new ADMX files reside by default on the local system drive of Windows Vista and Windows Server 2008 computers. The path to these ADMX files is C:\Windows\PolicyDefinitions.

## ADMX Repository

In conjunction with the changes to the administrative template file structure and formatting, another major change has occurred with the management of the administrative template files. A repository has been created and coded so that all ADMX files can now reside in one location, instead of being spread throughout the network on local computers.

The control and management of ADM templates was difficult and hard to manage, which is one of the major reasons for the change. Another key reason for the change is how ADM templates were handled within each GPO. Each GPO that was created copied the entire set of default ADM templates into the location where GPO settings were maintained (referred to as the Group Policy Template). The Group Policy template is located on domain controllers. Since there can be hundreds or thousands of GPOs, the space required to store these ADM templates was substantial. With each set of default ADM templates (coming in at a whopping 4MB of data) being stored on domain controllers, this could also add to replication traffic between domain controllers.

---

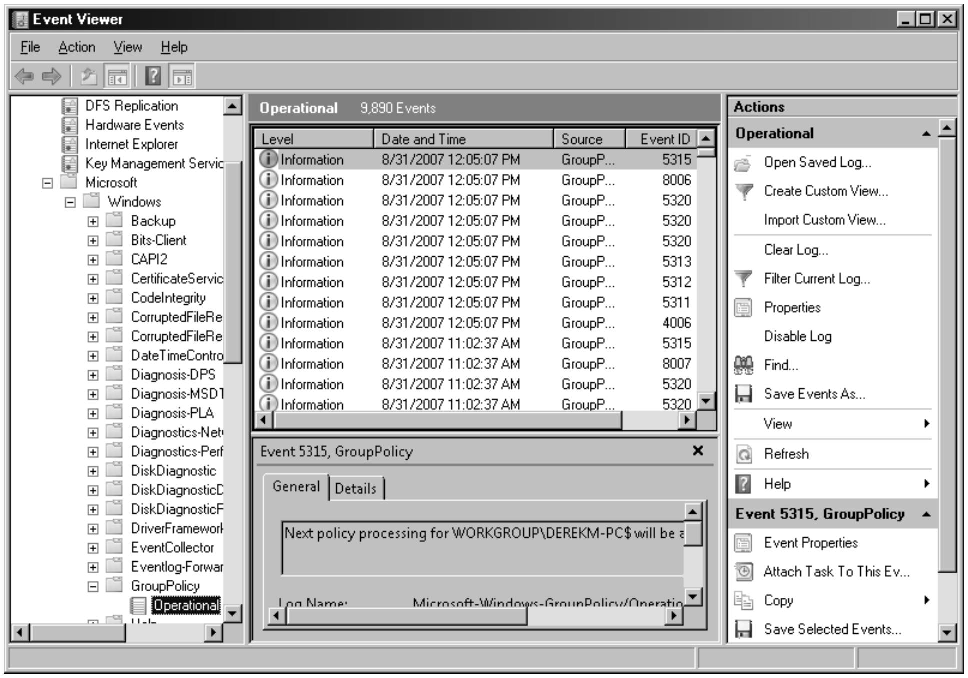
These negatives of ADM templates triggered the change and new technology to handle administrative template files. If no repository is created, the local ADMX files will still be used to edit a GPO. This keeps the administration of GPOs is consistent, even if the technology is not used. It should be noted, however, that the ADMX files are *not* stored in the Group Policy template. This change helps with storage of files on domain controllers, as well as the replication of those files between domain controllers.

> NoteADM template management and ADMX repository are described in detail in Chapter 9, "ADM, ADMX, and the ADMX Repository."

## Improved Logging

It is no secret that managing logging and documentation has been a struggle for Group Policy over the years. Trying to ferret out information from the old Event Log entries was a bit problematic. You needed to have a PhD in Group Policy and Microsoft to get much from the logging that occurred in the Event Viewer. The other logs, such as the userenv.log, were better, but still not ideal.

All of this has changed with the latest installment of GPO logging. The changes are like many of the other changes: stunning and fantastic. The new logging is built on the Event Log service that is available with Windows Vista. The new logging does away with the userenv.log and now stores information in a Group Policy Operational Log found in Event Viewer. You will find this log in Event Viewer by opening up the Applications and Services Logs, and then opening Microsoft\Windows\GroupPolicy\Operational. The resulting log view can be seen in Figure 2-6.



| Level | Date and Time | Source | Event ID |
|---|---|---|---|
| Information | 8/31/2007 12:05:07 PM | GroupP... | 5315 |
| Information | 8/31/2007 12:05:07 PM | GroupP... | 8006 |
| Information | 8/31/2007 12:05:07 PM | GroupP... | 5320 |
| Information | 8/31/2007 12:05:07 PM | GroupP... | 5320 |
| Information | 8/31/2007 12:05:07 PM | GroupP... | 5320 |
| Information | 8/31/2007 12:05:07 PM | GroupP... | 5313 |
| Information | 8/31/2007 12:05:07 PM | GroupP... | 5312 |
| Information | 8/31/2007 12:05:07 PM | GroupP... | 5311 |
| Information | 8/31/2007 12:05:07 PM | GroupP... | 4006 |
| Information | 8/31/2007 11:02:37 AM | GroupP... | 5315 |
| Information | 8/31/2007 11:02:37 AM | GroupP... | 8007 |
| Information | 8/31/2007 11:02:37 AM | GroupP... | 5320 |
| Information | 8/31/2007 11:02:37 AM | GroupP... | 5320 |

Next policy processing for WORKGROUP\DEREKM-PC$ will be a

Log Name: Microsoft-Windows-GroupPolicy/Operatio

**Figure 2-6** With the new logging that is available for Group Policy, new Group Policy events can be seen in the operational logs.

There are more benefits to using these new logs because they also provide specific new features that help with getting information out of the logs. The new logging technology provides for forwarding events to a central location; this is called *subscribing to an event*. Another benefit of the new log structure is the ability to filter views of specific events, making mining information from large log files more efficient.

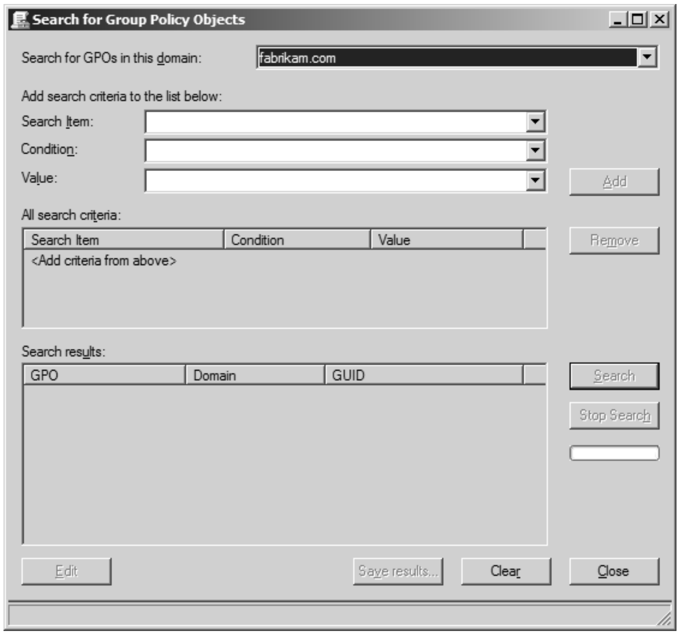
The is much more to logging. In Chapter 13, "Troubleshooting GPOs," you will get more information about logging.

## New Group Policy Features in Windows Server 2008

### Filters

If you have ever tried to decrypt the myriad settings that are in a GPO while trying to troubleshoot a problem, you know that it is a difficult task. With thousands of potential settings in a GPO, there has been very little with regard to filtering the settings, until now.

With Windows Server 2008, there is an entire platform for searching the settings in a GPO. The obvious search options are there, such as text searching for title, explanation text, and comments. These can be seen in Figure 2-7.



Search for GPOs in this domain: fabrikam.com

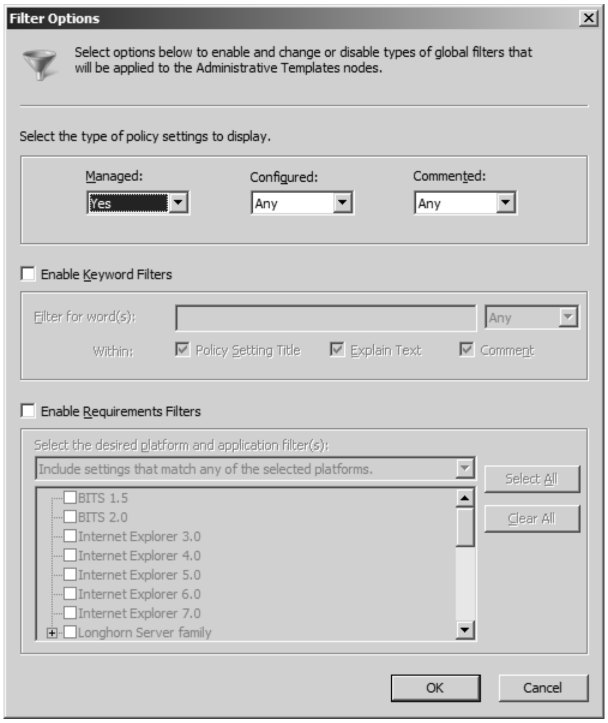
**Figure 2-7** The new filtering of GPO settings allows for basic searching and filtering of title, explanation text, and comments within a GPO.

Additional searching also exists that allows you to search based on operating system platform support. With so many iterations of Group Poilcy, as was discussed in Chapter 1, it is important to be able to pinpoint which settings work on which version operating system.

Another option for searching is based on which application and version is supported. With the different versions of Internet Explorer and Office, it is important to know which versions the Group Policy settings will affect.

For more information about the differences between how some Registry setting apply differently than other, see Chapter 10, “ADM, ADMX, and the ADMX Repository,” and Chapter 12, “Settings breakdown for Windows Server 2008 and Vista.” The difference is denoted as *managed* (policies) settings or *unmanaged*” (preferences) settings. With these Registy values making such a difference when applied and controlled, it is nice to be able to search for settings by category.

Finally, you can filter settings based on whether they are disabled or enabled. This is important when working with the new PolicyMaker technology settings. All of these configurations allow for the individual setting to either be enabled or disabled. The filter allows you to quickly see which settings in the GPO are configured, helping in troubleshooting and management alike. Figure 2-8 illustrates how filtering settings based on their enabled or disabled status can make your administrative efforts more efficient.


Filter Options

Select options below to enable and change or disable types of global filters that will be applied to the Administrative Templates nodes.

Select the type of policy settings to display.

Managed: Yes

Configured: Any

Commented: Any

☐ Enable Keyword Filters

Filter for word(s): Any

Within: ☑ Policy Setting Title ☑ Explain Text ☑ Comment

☐ Enable Requirements Filters

Select the desired platform and application filter(s):

Include settings that match any of the selected platforms.

**Figure 2-8** The new filtering options include the ability to search on enabled or disabled GPO settings.

## Starter GPOs

If you are the lead GPO administrator or responsible for those that create GPOs in your environment, you now have another tool in your toolbelt. The new Starter GPOs provide an excellent way for you to create a baseline of settings within an offline “Starter” GPO, which then can be copied to create a new GPO. The new GPO will contain all of the configurations and comments that were created in the Starter GPO.

The one small drawback to the Starter GPOs is that they can contain only Administrative Template settings. This is a bit limiting, but the ability to create a baseline of settings that can then be copied to create new GPOs is beneficial nonetheless. A sample Starter GPO can be seen in Figure 2-9.

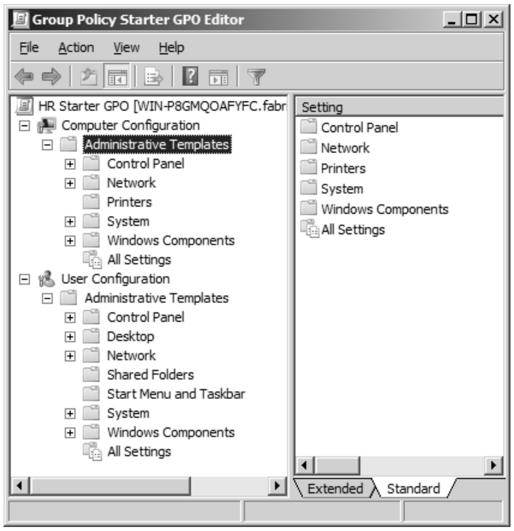


**Figure 2-9** Starter GPOs allow you to configure any setting falling under the Administrative Templates section of a GPO.

NoteIf you want to create baseline GPOs that contain settings from any portion of a GPO, you can use AGPM. AGPM allows you to create GPO templates, which are in essence Starter GPOs that contain all areas of a GPO.

Another benefit of Starter GPOs is the ability to include them in your RSoP analysis. This gives you an inside look at the settings that are in the Starter GPO, with regard to how they will interact with other GPOs that might have conflicting settings.

For more information on Starter GPOs refer to Chapter 6, "Using the GPMC."

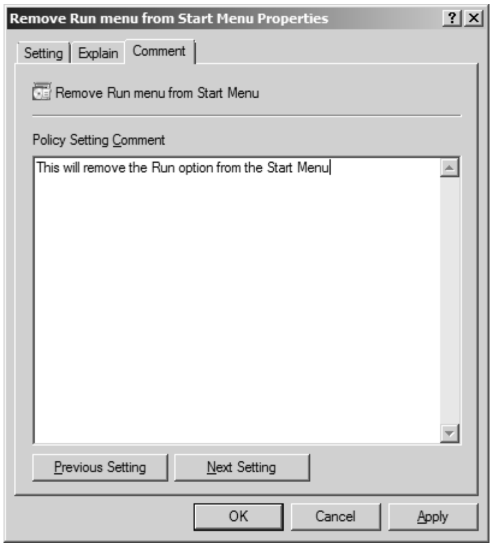
## Commenting

Changes to Group Policy Objects can have a large impact on the computers in the environment. A single change to a Group Policy setting can affect all computers in your company. With such a powerful tool such as Group Policy, some mechanism had to be developed to help maintain a documentation system for changes that occur to GPO settings.

One of those mechanisms is the ability to add comments to every GPO as a whole, as well as every GPO setting individually. This provides a more global and comprehensive way to track changes that occur to GPOs and their settings.

It is very common for changes to occur to GPOs that are caused by incidences on a computer. For example, an exploit might come about that is fixed by an Internet Explorer setting or a custom Registry entry. Changes like these usually occur quickly and without any documented reasoning. The outcome of this is future audits or analysis are left wondering why the change occurred.

With commenting, all changes are tracked immediately when the modification to the GPO occurs. This provides a very detailed trail of the changes that occur to GPOs throughout its life. Sample comments can be seen in Figure 2-10.


Remove Run menu from Start Menu Properties
Setting
Explain
Comment
Remove Run menu from Start Menu
Previous Setting
Next Setting
OK
Cancel
Apply

Policy Setting Comment: This will remove the Run option from the Start Menu

**Figure 2-10** A GPO can include comments, allowing for administrators to document the changes that occur each time the GPO is altered.

Not all comments are created equal though. The comments that are added to a new Starter GPO are not saved when a new GPO is created from that Starter GPO. The comments that are being referred to here are at the GPO level. The comments that are associated with the settings within the Starter GPO are saved and carried along to the new GPO.

This commenting mechanism is built this way to help senior administrators document information and details within the GPO for junior administrators that might use the Starter GPO to make a new GPO. Since the new GPO will carry along the settings configured in the Starter GPO, the comments associated with the settings go along with the GPO.

## So, What about Those DesktopStandard Products?

In late 2006, Microsoft acquired many of the tools and employees from DesktopStandard. The acquisition was extremely valuable for the entire Group Policy landscape. The tools and products that DesktopStandard had to offer were leaders in the industry. These tools are now available in a variety of different offerings by Microsoft.

### PolicyMaker

At the time of this writing, the PolicyMaker technology is scheduled to be delivered to the market in early to mid 2008. This falls in line with the release of Windows Server 2008, which is scheduled for early 2008.

As for the technology and offerings that PolicyMaker technology will provide, the majority of that information will be in Chapter 12, which is dedicated to PolicyMaker technology. However, there needs to be some introduction to PolicyMakerbecause it is a spectacular product and is coming with Windows Server 2008.

PolicyMaker technology will tie directly into the way that standard Group Policy is managed and controlled. You will use the Group Policy Management Console, Group Policy Object Editor, and Advanced Group Policy Management, just like you do today.

PolicyMaker technology contributes 22 client-side extensions to a GPO. These client side extensions include settings related to files, folders, user accounts, local groups, drive mappings, printer mappings, and much more.

PolicyMaker provides control over areas of a desktop and server that default Group Policy doesn't. The technology has been on the market for many years and customers have loved what it can do for them. Instead of going on and on here, if PoilcyMaker technology is something that could benefit you, Chapter 12 is where you should be looking now.

### Advanced Group Policy Management (GPOVault)

The other product line that Microsoft acquired along with PolicyMaker technology from DesktopStandard is Advanced Group Policy Management (AGPM). You might know this product from when it was owned by DesktopStandard. It was named GPOVault back then.

This product is offered a bit different than the other Group Policy products and technologies. AGPM is offered through the Microsoft Desktop Optimization Pack (MDOP). MDOP is only available to those companies that have bought software assurance. MDOP is a enormous package that offers a great "bang for your buck."

> NoteFor more information on MDOP, refer to *http://www.microsoft.com/windows/products/windowsvista/enterprise/mdopoverview.mspx*.

AGPM itself brings tremendous value to the Group Policy management arena. Although Chapter 8 goes into the AGPM features and settings in full detail, the following is a list of benefits that AGPM can provide to your GPO management environment.

- Role Based Delegation
- Rollback and rollforward to any GPO in the archive
- Offline Editing of GPOs
- Settings Difference Reports between two GPOs
- Workflow for GPO management tasks
- GPO Templates for baseline configurations
- Built on Group Policy Management Console (GPMC)
- Integrated Change Control for your Group Policy management environment

Some of these tasks can be completed using the GPMC and scripting, but AGPM performs these tasks seamlessly and automatically. AGPM is also a very lightweight installation, relying on a simple flat file structure and metadata to keep track of all of the changes within each GPO.

## Summary

With every new operating system comes new changes in every technology area. Group Policy is no different. There are some exciting and amazing new technologies with Windows Vista and Windows Server 2008. Some of these technologies were introduced with Windows Vista, including local GPOs, Network Location Awareness, logging improvements, ADMX file format, and ADMX repository. New for Windows Server 2008 are many updates to GPMC, including searching, commenting, and filtering, as well as PolicyMaker technology. Last and not least, is the new AGPM functionality which makes management of Group Policy easier and more efficient.

# Additional Resources

- Microsoft Group Policy Website, at *http://www.microsoft.com/grouppolicy*, includes more information on the new features and settings that are available in Windows Server 2008 and Windows Vista
- Microsoft TechNet Website, at *http://technet2.microsoft.com/WindowsVista/en/library/9c7ecc7d-8784-4b8d-ba1f-ba1882ba83741033.mspx?mfr=true* titled "Step-by-Step Guide to Managing Multiple Local Group Policy Objects", includes more information on multiple local Group Policy objects in Windows Vista.
- Chapter 14, "Advanced Group Policy Management with AGPM", includes information about installing AGPM, how to use AGPM, how to obtain AGPM, and the benefits of AGPM.
- Chapter 13, "Settings Breakdown for Windows Server 2008 and Windows Vista", includes information about specific settings within a GPO.
- Appendix A, "Third Party Tools", includes information about other companies that have extended Group Policy.
- MLGPO overview and step-by-step guide at *http://technet2.microsoft.com/WindowsVista/en/library/9c7ecc7d-8784-4b8d-ba1f-ba1882ba83741033.mspx?mfr=true*