



Global Knowledge™

Expert Reference Series of White Papers

# Windows Server 2008 and New Group Policy Settings

# Windows Server 2008 and New Group Policy Settings

Glen Weadock, Instructor and Course Developer, MCSE, MCSA, A+



## Introduction

Group Policy puts an impressively powerful toolset into the hands of administrators working in the Active Directory environment. The Group Policy Object Editor (GPOE) acts much like a centralized, network-aware Registry editor: Make a setting, and Group Policy enforces it for you from that point forward. (Of course, Group Policy goes beyond Registry settings to include a variety of security and software installation capabilities, too.)

Group Policy is highly flexible. You can deploy different Group Policy settings, based on Organizational Unit (OU), domain, or site, and (with a little sleight of hand) Windows group membership, through a Group Policy technique called security group filtering.

With the advent of Microsoft's Windows Server 2008 technologies – that is, Windows Vista on the client and Server 2008 on the server side – comes a wealth of new and improved Group Policy settings: approximately 700, in fact! Some of these settings are in entirely new categories; others are additional, corrected, or more convenient settings in existing categories.

Some of the more interesting new categories include:

- Network Access Protection
- Device installation control
- Removable storage restrictions
- Power management
- Printer driver installation delegation
- Hybrid hard disk
- Troubleshooting and diagnostics
- User Account Control

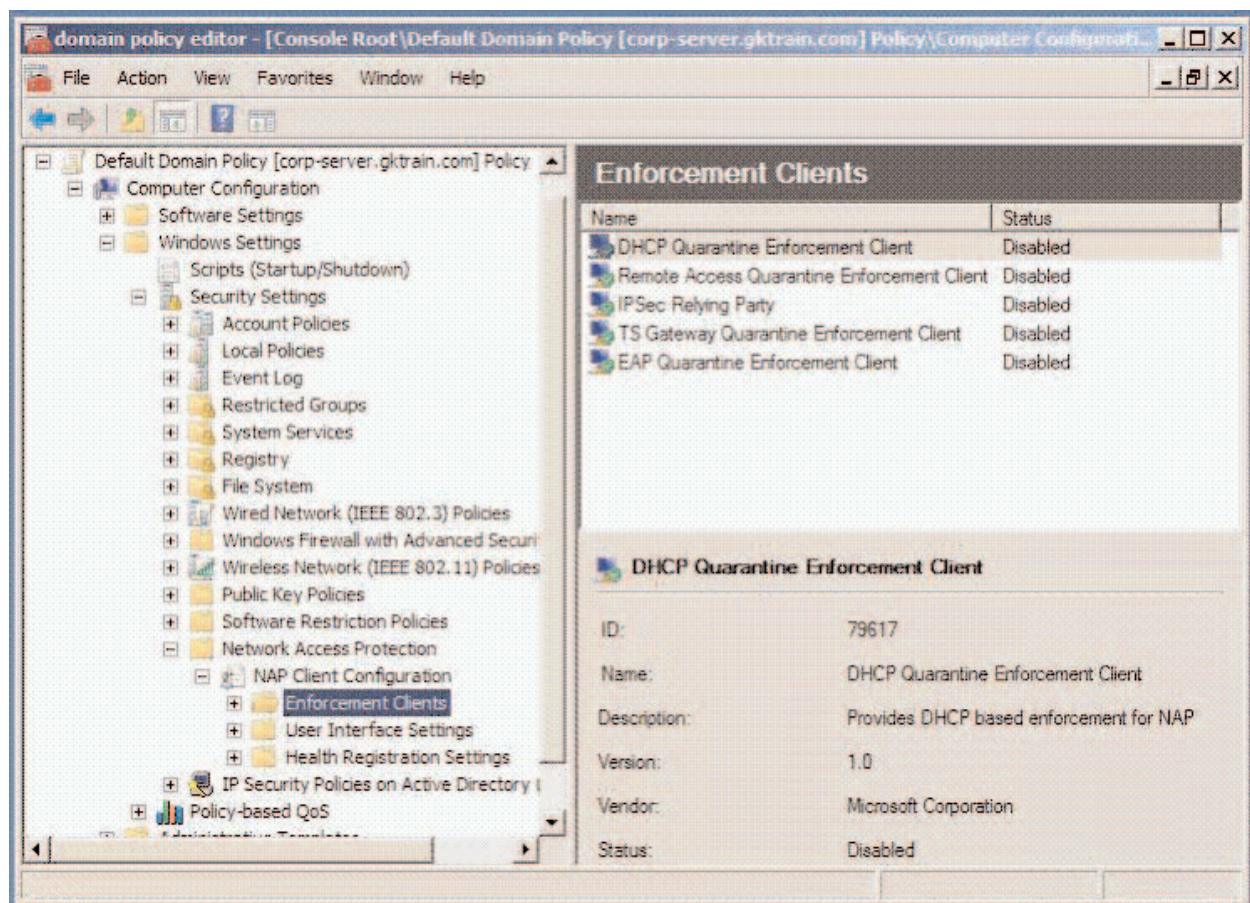
Changes and additions to existing categories include:

- IPsec and firewall
- AD-based printer deployment
- Taskbar and Start menu
- Shell visualization
- Synchronization scheduling
- Customized help resources

This paper takes an introductory look at the new categories, but anyone moving to Windows Server 2008 technologies would do well to consider the changes and additions to the existing policy categories, too. A Microsoft spreadsheet listing all the new and changed policy settings for Windows Werver 2008 may be found by searching for the file VistaGPSettings.xls at [www.microsoft.com](http://www.microsoft.com).

**NOTE:** Before diving in to discuss the new settings, you should be aware of a change in the way Windows Server 2008 and Vista store Group Policy settings. The venerable ADM file format has given way to a new format, ADMX, which offers a number of benefits, including central-store management on domain controllers, multi-language support, and dynamic loading. Vista or Windows Server 2008 Server is required to read ADMX files. You can obtain an ADM-to-ADMX migration tool from Microsoft at no charge (search for the phrase "ADMX Migrator").

## Network Access Protection



**Figure 1. The NAP policy user interface is informative but non-standard.**

**Location: Computer Configuration > Windows Settings > Security Settings > Network Access Protection**

**Note:** You must be viewing a network Group Policy Object (GPO) in order to see the above location; it does not appear when viewing a local GPO. All screenshots in this white paper are from a functioning Windows Server 2008, but you will see many similar, if not identical, settings in Vista.

Network Access Protection (NAP) is an attractive security capability of Vista in combination with at least one Windows Server 2008. NAP lets administrators set conditions under which workstations are allowed to connect to the main network. For example, a laptop user who turned off her firewall over the weekend will not be granted access Monday morning until she turns the firewall back on. Or, even better, the NAP client will automatically turn the firewall back on without her intervention: something called "auto-remediation."

NAP also provides for the automatic redirection of "unhealthy" clients to a separate subnet or subdomain, where they could, for example, download security updates in order to bring themselves into compliance with the health policies. System health policies can be enforced by DHCP (Dynamic Host Configuration Protocol) running on Windows Server 2008 for clients accessing the network locally, and by the RRAS (Routing and Remote Access) service for clients accessing the network remotely. Third-party antivirus software vendors are expected to create agents that can extend NAP to include rules for updated virus signatures.

The Group Policy settings for NAP include the following:

- Which enforcement clients you want to run;
- The way the NAP client should appear (you can specify custom text and a custom image); and
- So-called "health registration" settings which specify the encryption methods that clients can use to communicate with Health Registration Authority servers, if you're using certificates.

We can't begin to cover this subject in the depth that it deserves, but soon there will be another Global Knowledge white paper dedicated to this subject.

## Device Installation Control

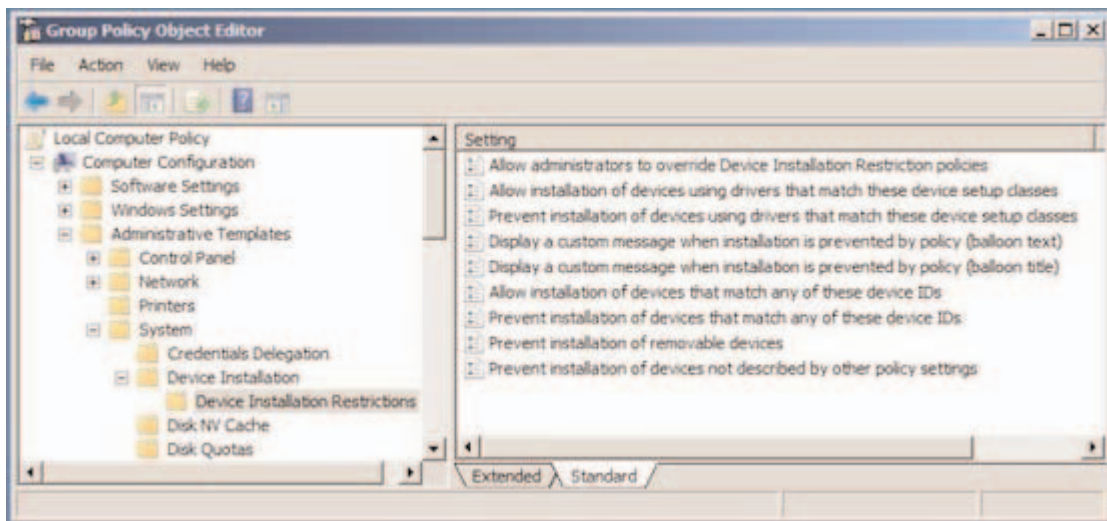


Figure 2. Here, you can manage who can install what kinds of devices.

### Location: Computer Policy > Administrative Templates > System > Device Installation > Device Installation Restrictions

IT administrators may occasionally wish to restrict the use of flash drives (also known as thumb drives) in the computing environment. While this category doesn't let you disable the use of such devices entirely – see the

"Removable Storage Restrictions" section below – this category does allow you to control the installation of device drivers, based on setup class.

For example, with this category of policy settings, administrators could define a "driver store" of known good, safe drivers that any user, regardless of account type, will be permitted to install and use.

You must determine the device setup class or specific device ID in order to use this feature, depending on which specific policy setting you want to use (don't mix them up). The device setup class is in the form of a GUID (Globally Unique Identifier). So, how do you figure out the right GUID to use? The Device Manager's Details tab lets you do that. Under "Property," you can choose from the drop-down menu to see the device ID and/or the setup class IDs.

**TIP:** Often there will be multiple IDs you can use, some more specific than others. Use this feature to your advantage, depending on how precisely you need to prohibit the installation of a particular device driver or class of device drivers.

## Removable Storage Restrictions

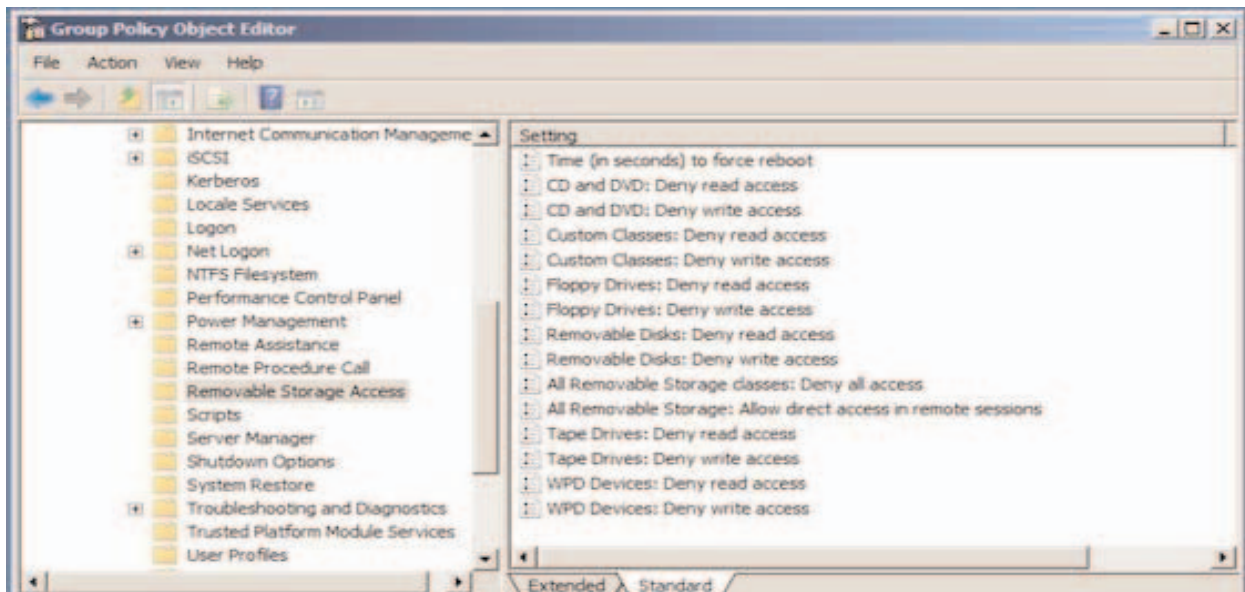


Figure 3. Securing those pesky removable devices.

### Location: Computer Configuration > Administrative Templates > System > Removable Storage Access

With these policies, you can deny read access, write access, or both, to the following device types:

- CD and DVD
- Floppy drives (remember those?)
- Removable disks (presumably, other than CD and DVD)
- Tape drives
- WPD devices (media players, cell phones, PDAs, etc.)

- Custom classes (which you can define by device GUID)
- All of the above

In summary, you can use Device Manager to discover the GUIDs for the specific devices you wish to restrict using the "custom classes" option. Note that if you disable all removable storage devices, you can come back and permit access to removable storage devices in remote sessions.

## Power Management

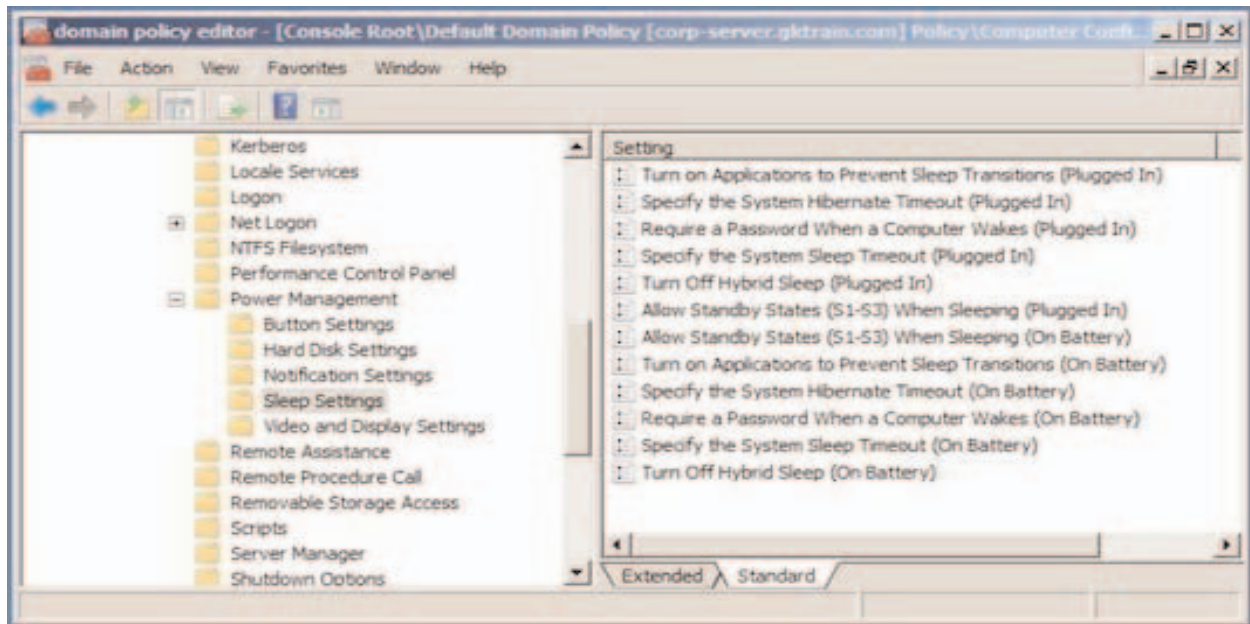


Figure 4. You now have the power to manage power.

### Location: Computer Configuration > Administrative Templates > System > Power Management

In previous versions of Windows, it was necessary to go to third parties if you needed to install policies that controlled the power-management features of networked systems (for example, [www.energystar.gov](http://www.energystar.gov) offered a tool called EZ GPO for this purpose).

Now, in Windows Vista, you can control power management settings for the power button (or buttons), laptop lid switch, hard drive, display, and sleep mode (a new mode that combines features of the old standby and hibernate modes). Additionally, you can create a custom plan for deployment to computers, or you can specify which of the three "canned" Microsoft power plans should be made the default active plan. You can also tweak the notifications that users receive in low battery situations.

Windows Server 2008- and Vista-aware workstations may have multiple power-related buttons: power, sleep, and the lid switch that closes when you close a laptop display. In addition, the Vista and Windows Server 2008 Start menus have their own power buttons, which are also separately configurable via Group Policy.

## Printer Driver Installation Delegation

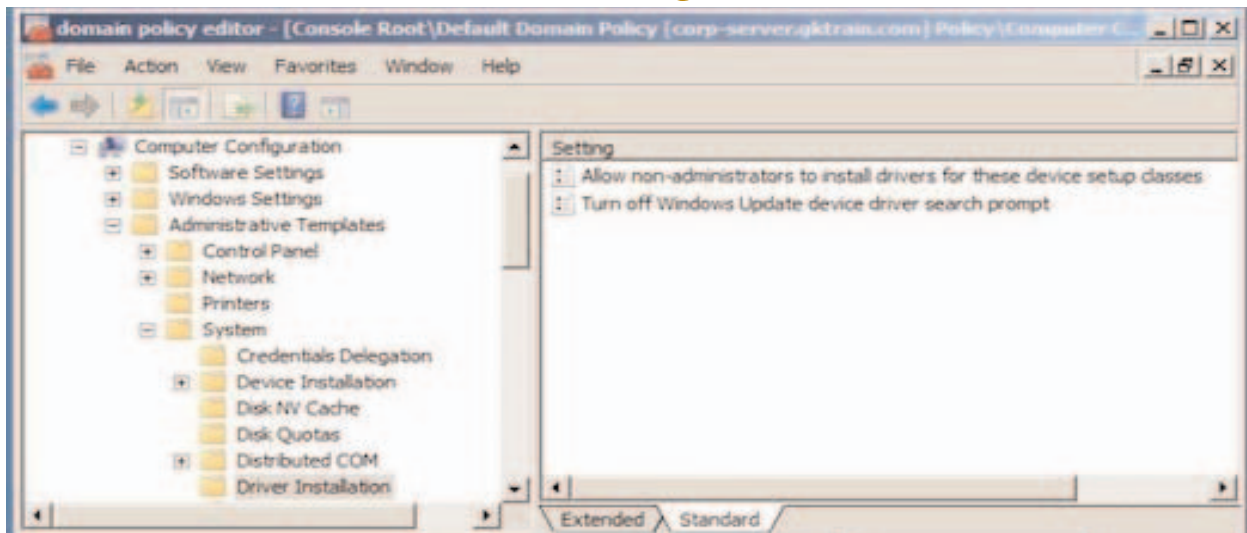


Figure 5. Delegating device installation privileges via Group Policy.

**Location: Computer Configuration > Administrative Templates > System > Driver Installation > Allow non-administrators to install drivers for these device setup classes**

One policy doesn't really make a category, but this one is useful enough to deserve separate mention.

One of the difficult aspects of moving away from users having administrative rights on their local machines is the knotty problem of printer driver installation. Typically, limited or standard users can't install printer drivers, only administrators can. The same is true of a wide range of other device types. In Windows Server 2008, you can delegate the ability for members of the Users group to install devices of a particular setup class. Once again, you'll need the GUID for the setup class of interest.

One caveat is that this policy only works for signed device drivers. Unsigned drivers will still generally need to be installed by administrators.

## Hybrid Hard Disk

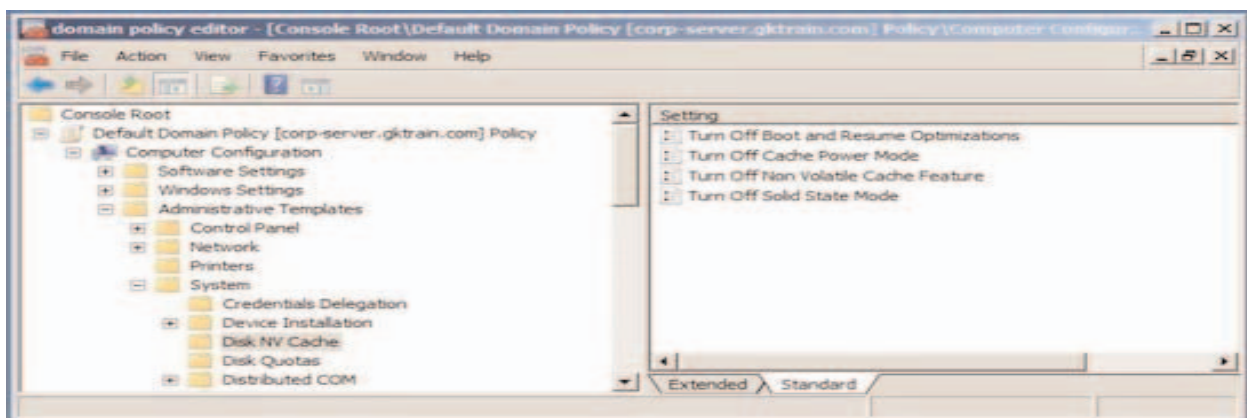


Figure 6. Controlling the nonvolatile cache in hybrid hard drives.

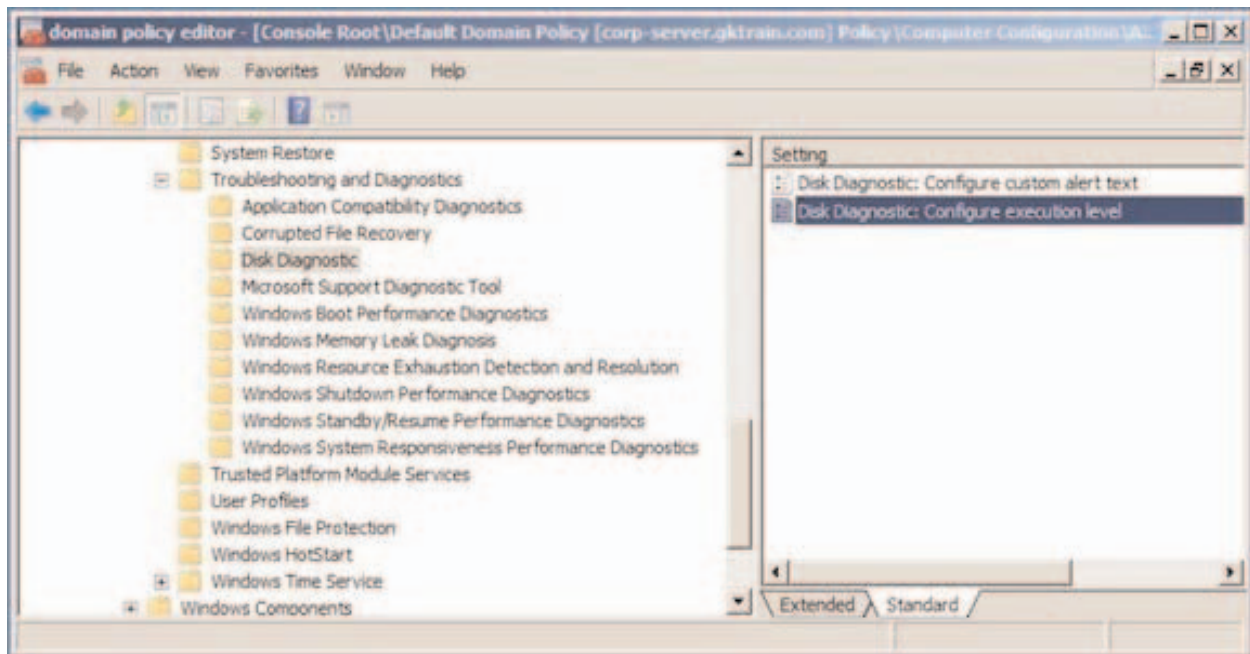
**Location: Computer Configuration > Administrative Templates > System > Disk NV Cache**

The hybrid hard disk (HHD) is a new device type being co-developed by Microsoft and Samsung (and others too, although it's not clear how broadly the policy settings will apply to other designs, such as Intel's). The idea is to combine a traditional magnetic spinning-disk device with non-volatile semiconductor storage (flash memory). It's a "hybrid" because it slots somewhere between spinning disks (cheap and ubiquitous) and pure solid-state disks (expensive and rare).

The Group Policy settings give you the ability to turn the non-volatile (NV) cache off entirely. You can also selectively turn off the feature, whereby the disk writes boot-and-resume data to the NV cache during shutdown or hibernate, for faster boot or resume. Additionally, you can turn off the feature whereby the disk goes into a power-saving mode by spinning down the magnetic disk and meeting I/O requests from the NV cache. Finally, you can disable the feature that stores registry writes in the NV cache ("solid-state mode").

Generally, the default settings (that is, Group Policy settings "not configured") give the best speed. Organizations moving to HHDs may wish to start deploying them while using Group Policy to restrict the feature set until full testing of all features is complete.

## Troubleshooting and Diagnostics



**Figure 7. Managing Windows Server 2008's new diagnostic capabilities.**

**Location: Computer Configuration > Administrative Templates > System > Troubleshooting and Diagnostics**

Windows Server 2008 and Vista provide a number of new troubleshooting and diagnostics tools to tailor the new diagnostic capabilities built into these platforms (primarily, the Diagnostic Policy Service or DPS). For example, unlike XP and Server 2003, the operating system checks S.M.A.R.T. (Self Monitoring Analysis and Reporting Technology) hard drives once per hour for potential warning signs; with Group Policy, you can specify whether you want the OS to merely log an event, or also alert the user.

Many of the settings in this category have the name "Configure Scenario Execution Level." Generally, you have two choices: Detection and Troubleshooting Only, or Detection, Troubleshooting, and Resolution. The latter involves a user notification as well as an event log entry. You can either configure this setting at the overall level, which applies to all the diagnostic and troubleshooting categories, or leave the overall setting "not configured" and make individual settings for each troubleshooting category.

Be aware that most of the troubleshooting and diagnostics settings only have an effect if DPS is actually running on the machine receiving the policy.

## User Account Control

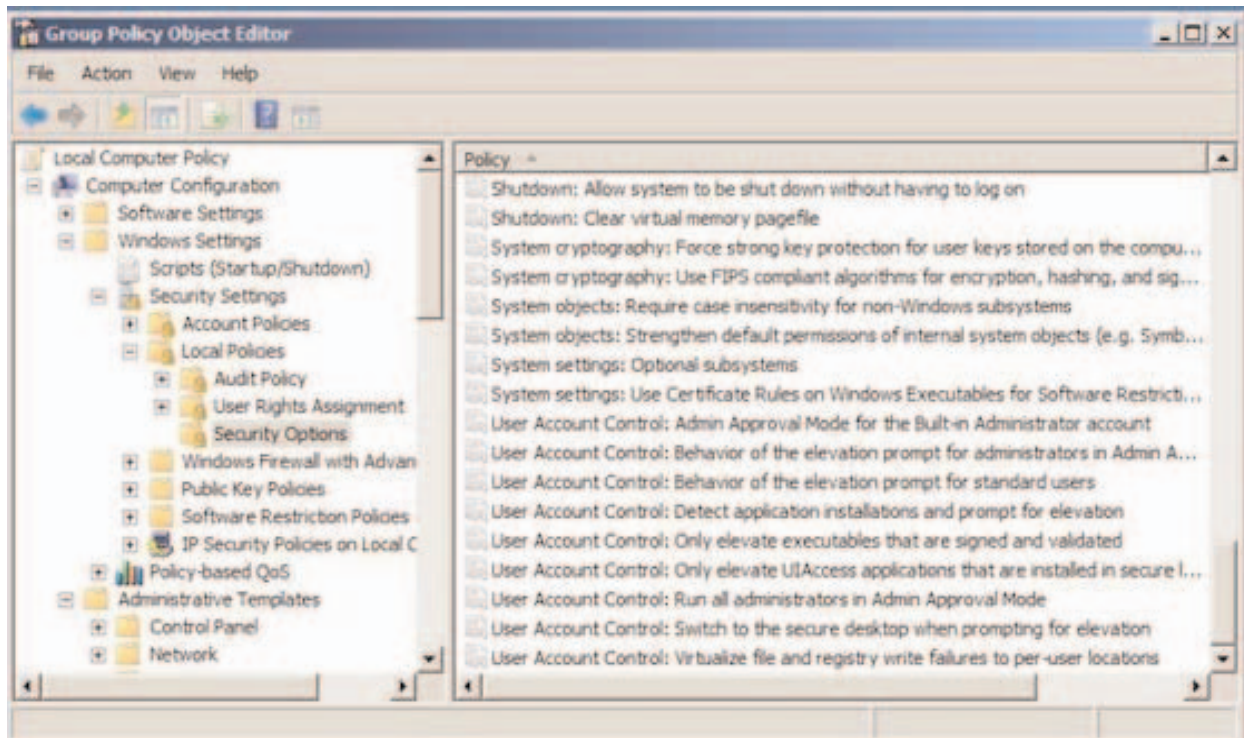


Figure 8. You decide how much (if any) of UAC you want to implement.

**Location: Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options (then scroll down to the U's)**

User Account Control (UAC) was developed to address concerns that viruses and malware can do much more damage to a system when a user is logged on with administrative rights on the local machine, than when the user is logged on as a limited or "standard" user. With UAC turned on, even when you are logged on as a local administrator, you do not normally execute processes with administrative privileges.

If you try to perform an action that does require such privileges, UAC prompts you for confirmation, before elevating your privileges. If you are logged on as a standard user, and you try to do something that requires admin rights, by default, you will be prompted to provide credentials of an account that has such rights. The

idea is to prevent rogue software from doing things you don't want it to do – and, incidentally, to make administrators stop and think for a second before executing potentially damaging tasks.

You can change this behavior through Group Policy so that non-administrators are simply denied, rather than prompted for, credentials. You can modify UAC prompt behavior for the built-in Administrator account, as opposed to other non-built-in accounts that you create and make part of the Administrators group. And you can turn UAC completely off, if you find that the bother outweighs the benefit.

One little setting in this category has an intriguing name: "Virtualize file and registry write failures to per-user locations." This is on by default, and it allows Vista and Windows Server 2008 to provide greater compatibility with legacy applications by redirecting certain kinds of writes that are now forbidden (such as to C:\Program Files) to special locations in the user profile, to avoid program errors. I'm not quite sure why it's under UAC, nor can I imagine why anyone would want to turn it off, but it is worth a mention.

## Conclusion

Group Policy just keeps getting bigger and more powerful. The new categories of GP settings in the client and server Windows Server 2008 platforms seem to be eminently useful and practical. The only downside is that we now have a few hundred more settings to learn – as well as some other "architectural" Group Policy advances, like Network Location Awareness, improved log file viewing, and GP's new status as a full-fledged service instead of a thread within the Winlogon service. But those topics will have to wait for the next white paper!

## Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge.

Check out our complete Microsoft curriculum at [www.globalknowledge.com/training/microsoft.htm](http://www.globalknowledge.com/training/microsoft.htm).

For more information or to register, visit [www.globalknowledge.com](http://www.globalknowledge.com) or call 1-800-COURSES to speak with a sales representative.

Our courses and enhanced, hands-on labs offer practical skills and tips that you can immediately put to use. Our expert instructors draw upon their experiences to help you understand key concepts and how to apply them to your specific work situation. Choose from our more than 700 courses, delivered through Classrooms, e-Learning, and On-site sessions, to meet your IT and management training needs.

## About the Author

Glenn Weadock is a long-time instructor for Global Knowledge and co-course-director with Mark Wilkins of the seminars Implementing and Maintaining Microsoft Windows Vista, Migrating to Windows Vista, and Deploying Group Policy. He also consults through his Colorado-based company Independent Software, Inc. and is the author of 18 computer books.