

Top Seven Tips and Tricks for Group Policy in Windows 7

Written by
Jeremy Moskowitz, Microsoft Group Policy MVP, GPanswers.com

© 2010 Quest Software, Inc.

ALL RIGHTS RESERVED.

This document contains proprietary information protected by copyright. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose without the written permission of Quest Software, Inc. ("Quest").

The information in this document is provided in connection with Quest products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest products. EXCEPT AS SET FORTH IN QUEST'S TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software World Headquarters

LEGAL Dept

5 Polaris Way

Aliso Viejo, CA 92656

www.quest.com

E-mail: **legal@quest.com**

Refer to our Web site for regional and international office information.

Trademarks

Quest, Quest Software, the Quest Software logo, AccessManager, ActiveRoles, Aelita, Akonix, AppAssure, Benchmark Factory, Big Brother, BridgeAccess, BridgeAutoEscalate, BridgeSearch, BridgeTrak, BusinessInsight, ChangeAuditor, ChangeManager, Defender, DeployDirector, Desktop Authority, DirectoryAnalyzer, DirectoryTroubleshooter, DS Analyzer, DS Expert, Foglight, GPOAdmin, Help Desk Authority, Imceda, IntelliProfile, InTrust, Invirtus, iToken, I/Watch, JClass, Jint, JProbe, LeccoTech, LiteSpeed, LiveReorg, LogAdmin, MessageStats, Monosphere, MultSess, NBSpool, NetBase, NetControl, Npulse, NetPro, PassGo, PerformaSure, Point,Click,Done!, PowerGUI, Quest Central, Quest vToolkit, Quest vWorkSpace, ReportAdmin, RestoreAdmin, ScriptLogic, Security Lifecycle Map, SelfServiceAdmin, SharePlex, Sitraka, SmartAlarm, Spotlight, SQL Navigator, SQL Watch, SQLab, Stat, StealthCollect, Storage Horizon, Tag and Follow, Toad, T.O.A.D., Toad World, vAutomator, vControl, vConverter, vFoglight, vOptimizer, vRanger, Vintela, Virtual DBA, VizionCore, Vizioncore vAutomation Suite, Vizioncore vBackup, Vizioncore vEssentials, Vizioncore vMigrator, Vizioncore vReplicator, WebDefender, Webthority, Xaffire, and XRT are trademarks and registered trademarks of Quest Software, Inc in the United States of America and other countries. Other trademarks and registered trademarks used in this guide are property of their respective owners.

January 2010

Contents

Introduction.....	3
Tip #1: Use a Windows 7 Management Machine.	4
Tip #2: Manage Windows 7's Power Using Policy Settings and Controls for "Power Plan" Preferences	6
Tip #3: Lock Out Unwanted Hardware Using Group Policy.....	9
Tip #4: Note that the "Immediate Task" Function for Windows 7 Machines Doesn't Work Yet.....	10
Tip #5: Use PowerShell to Deploy Scripts	12
Tip #6: Use PowerShell for Scripting Group Policy Operations.....	13
Tip #7: Get Application-level Control Using AppLocker.....	15
Conclusion.....	17
About the Author	18

Introduction

Windows 7 comes with a host of new features. In corporate environments, the last thing IT departments want is for users to have free rein over these new features once Windows 7 is deployed to their desktops.

Group Policy is the de facto way to deploy security settings and desktop settings and ensure a complete lockdown. IT support and IT managers can utilize the Group Policy infrastructure they already have to ensure compliance with corporate standards and company settings.

In this document, we'll examine the top seven Group Policy tips and tricks for Windows 7. You'll learn about the new features, what works, what doesn't, and how to make the most of your Windows 7 investment.

Tip #1: Use a Windows 7 Management Machine.

This tip is the foundation for all the other tips in this document. In order to make the most of the new Group Policy functionality in Windows 7, you'll need to commit to having one "management machine" running Windows 7. Alternatively, you could use a Windows Server 2008/R2 machine as your management machine, but for practical purposes, most administrators will likely use Windows 7.

Once you've chosen your Windows 7 management machine, you'll need to install the Group Policy Management Console (GPMC) to have access to all the new features. However, the GPMC is not "in the box"; it's available only as part of a downloadable package called Remote Server Administration Toolkit (RSAT). Therefore, the first step in creating a Windows 7 management machine is to download RSAT and install the GPMC component.

Trying to find the RSAT for Windows 7 can be a bit of a challenge, so here's a URL you can use to download it: <http://tinyurl.com/klycep>. If that link changes, search for the phrase "Remote Server Administration Tools for Windows 7."

Note that there are both 32-bit and 64-bit versions, so be sure to install the correct one for your architecture. Also, beware of downloading older "RC" (Release Candidate) and beta versions of RSAT.

Once RSAT is installed, you can select **Remote Server Administration Tools** inside **Control Panel | Programs | Turn Windows Features on or off**, as shown below:

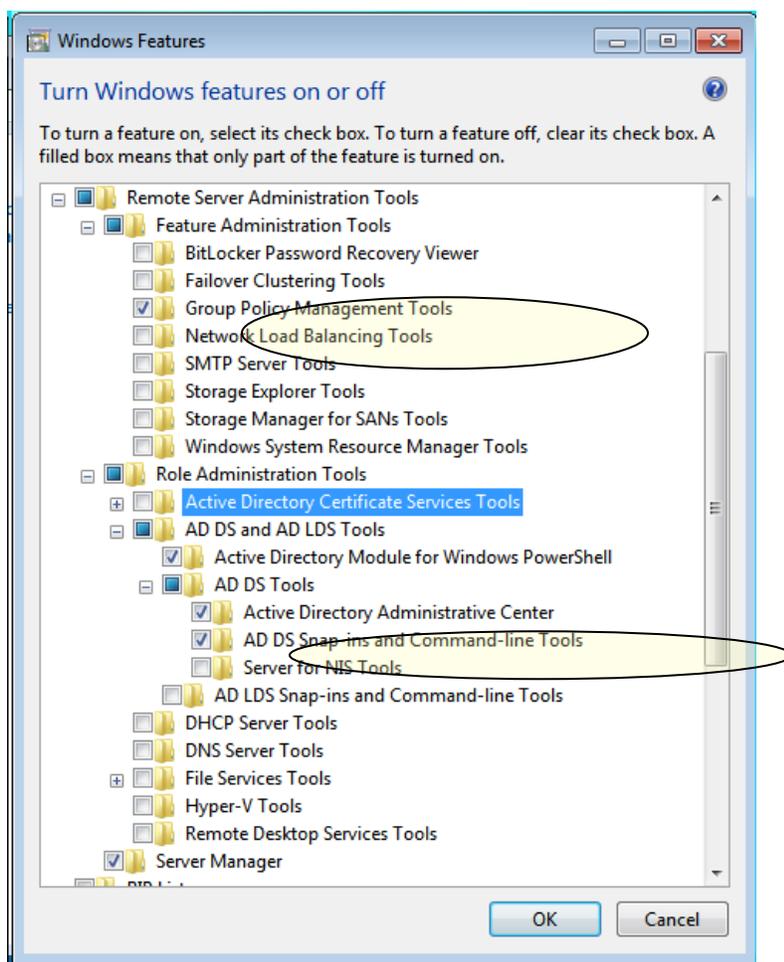


Figure 1. Installing RSAT adds the latest GPMC to Windows 7

Figure 1 shows how to select “Group Policy Management Tools” to install the GPMC and “Active Directory Administrative Center” to add Active Directory Users and Computers and other Active Directory–related tools.

Once installed, the GPMC is available by running GPMC.MSC from the command prompt, or locating it from the Start Menu.

Some items will have special Windows 7–only areas. For example, you may discover that items that worked fine in Windows Vista now have some extra control, such as the wireless policy highlighted in Figure 2.

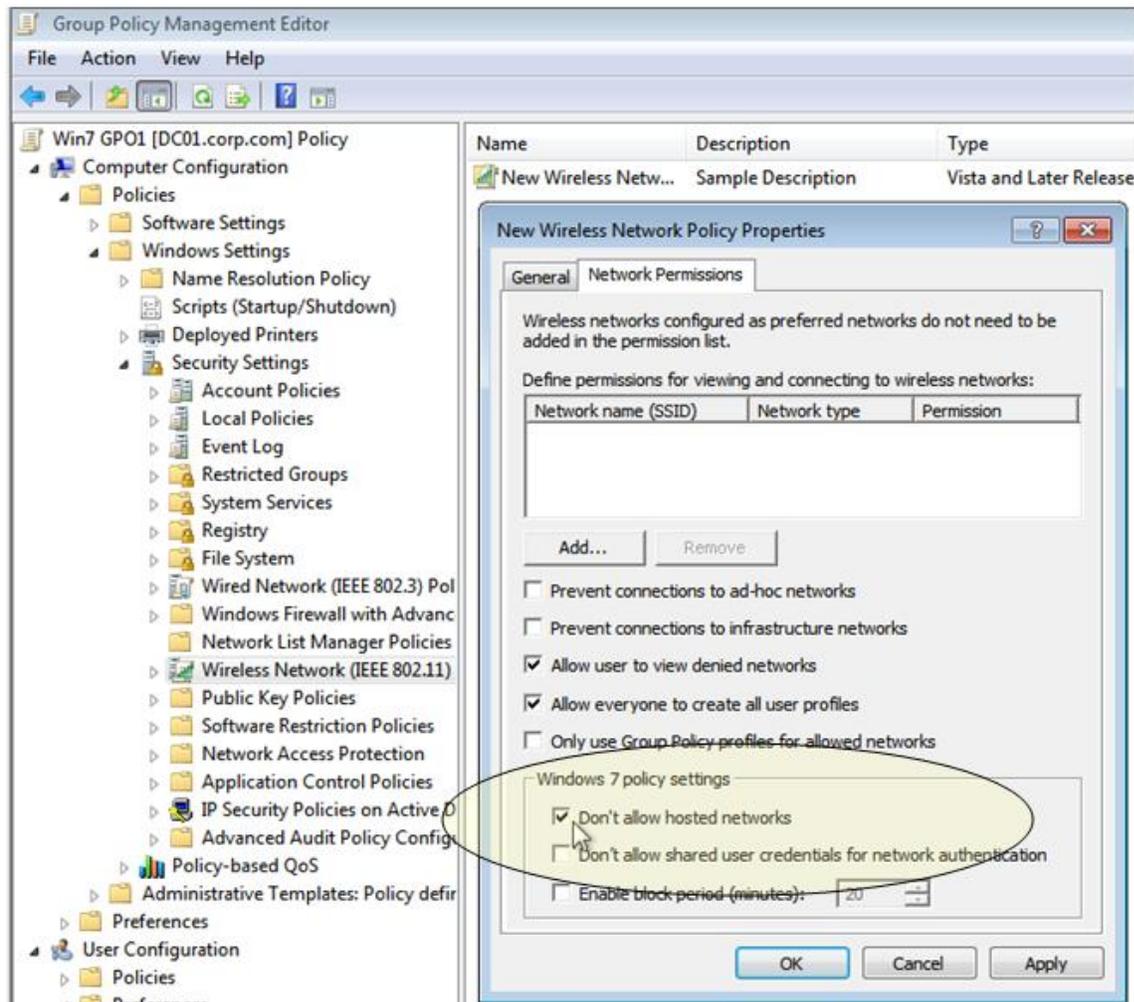


Figure 2. The updated RSAT with the GPMC on Windows 7 provides more Windows 7 controls.

Now that your Windows 7 management machine is up and running, you'll be able to deploy the 3000-plus Group Policy and Group Policy Preferences settings to your client machines to give them the appropriate user experience.

Tip #2: Manage Windows 7's Power Using Policy Settings and Controls for "Power Plan" Preferences

To lower your operational costs, use Group Policy to deliver settings that decrease the "power footprint" of your desktops and laptops. The smaller your power footprint is, the more money you will save—day after day, and year after year.

Power-related policy settings can be found at **Computer Configuration | Policies | Administrative Templates | System | Power Management**, as shown in Figure 3. Note that these policy settings are available only for computers, not users.

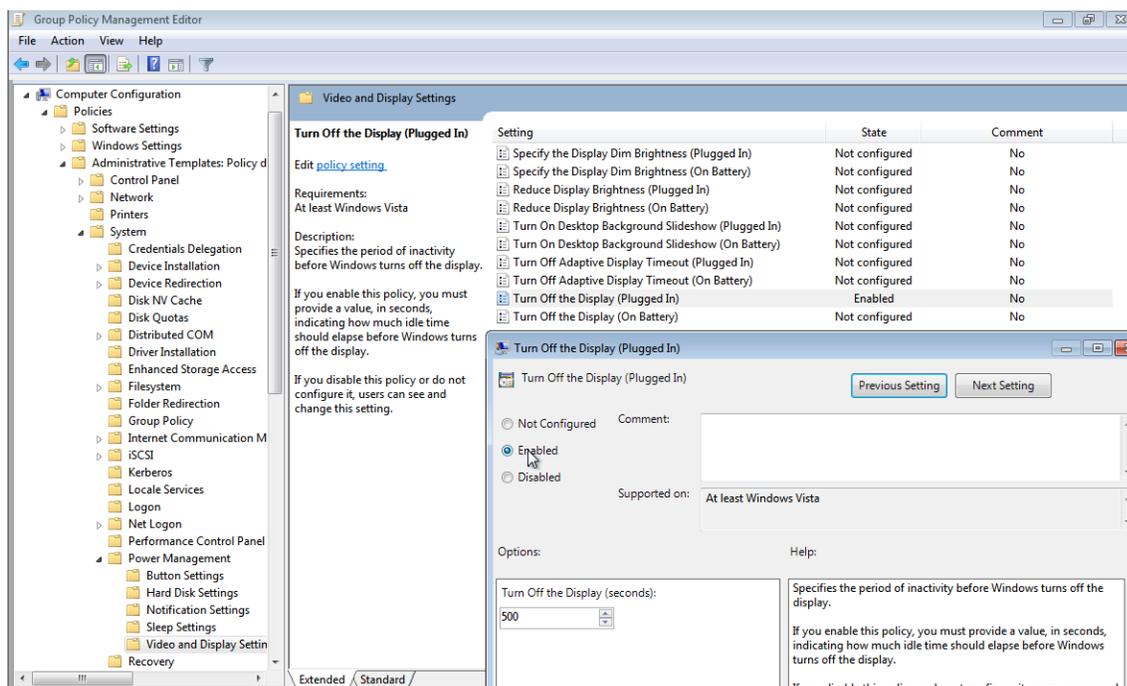


Figure 3. Use Group Policy Power Management settings to configure power-related policies for computers.

Also available are Group Policy Preferences settings for both users and computers. You can find those in **Computer Configuration | Preferences | Control Panel Settings | Power Options** and **User Configuration | Preferences | Control Panel Settings | Power Options**, as seen in Figure 4.

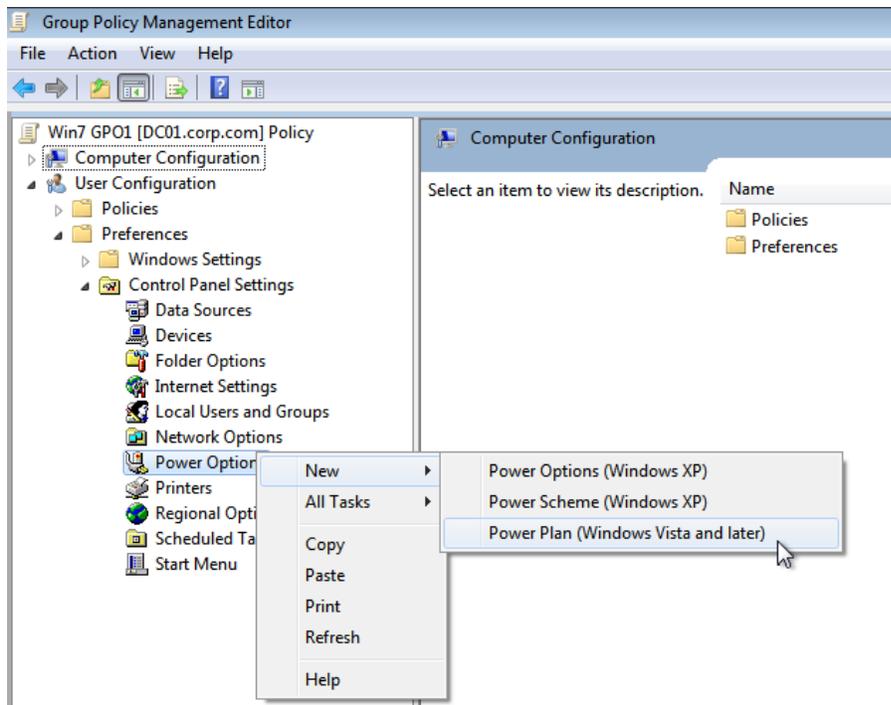


Figure 4. Group Policy Preferences for Windows 7 Power Plans are on both the computer and user sides.

The Group Policy Preferences for Power Plan settings (Figure 5) offer even more settings than the policy settings shown in Figure 3.

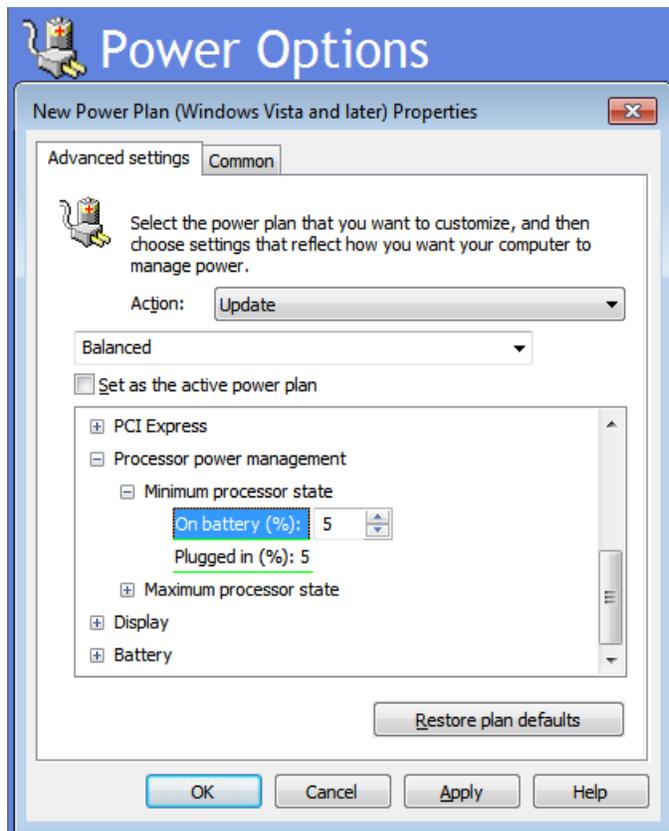


Figure 5. Use Group Policy Preferences' Power Settings to set even more power-specific savings.

However, remember that the nature of Group Policy preferences is different than Group Policy's policy settings: preferences can be undone by users at any time, while policy is enforced by the system and cannot be bypassed by regular users.

Also note that the Preferences item is named "Power Plan (Windows Vista and later)," which implies that configurations should be embraced by both Windows 7 and Windows Vista machines. As of now (Winter 2009/2010), that is not true; an upcoming Windows Vista update is in progress to address this issue. As soon as the update is released, there will be an announcement in the "Tip of the Week" newsletter at GPanswers.com.

By instituting power management settings using Group Policy and/or Group Policy Preferences, you'll immediately be able to recoup some of your Windows 7 deployment costs.

Tip #3: Lock Out Unwanted Hardware Using Group Policy

One of the key security concerns for administrators should be preventing corporate data from “walking away” from the network. For this reason, you may want to prevent items like USB flash drives, cameras and phones using flash media, or other kinds of hardware devices from being used on your network.

You can use Group Policy to:

- **Blacklist a specific device.** This ensures that specific hardware, such as a USB flash drive, cannot be used.
- **Whitelist specific devices.** Unless the device type is on the list, it is not permitted.

The policy settings that enable you to perform hardware lockout are located at **Computer Configuration | Policies | Administrative Templates | System | Device Installation | Device Installation Restrictions**. These hardware lockout policy settings are valid for Windows Vista and onward, including Windows 7.

You can see a live demonstration of how to perform device blacklisting by visiting to <http://tinyurl.com/ycrg46a> and watching a snip from the GPanswers.com “Group Policy University” training.

Tip #4: Note that the “Immediate Task” Function for Windows 7 Machines Doesn’t Work Yet

People often ask me if there’s a way to use Group Policy to reach out and touch all of their machines at once. You might want to do this, for example, to perform the same command on all machines at the same time or to set up a future event.

However, it is important to remember that the Group Policy engine itself is not “immediate.” The GPO on the domain controllers contains the “payload” of directions. Group Policy settings are pulled from that GPO every 90 minutes or so by the client.

One of those payloads can be a new instruction for Windows 7 and Windows Server 2008/R2 called an “Immediate Task”, as seen in Figure 6 with the payload seen in Figure 7.

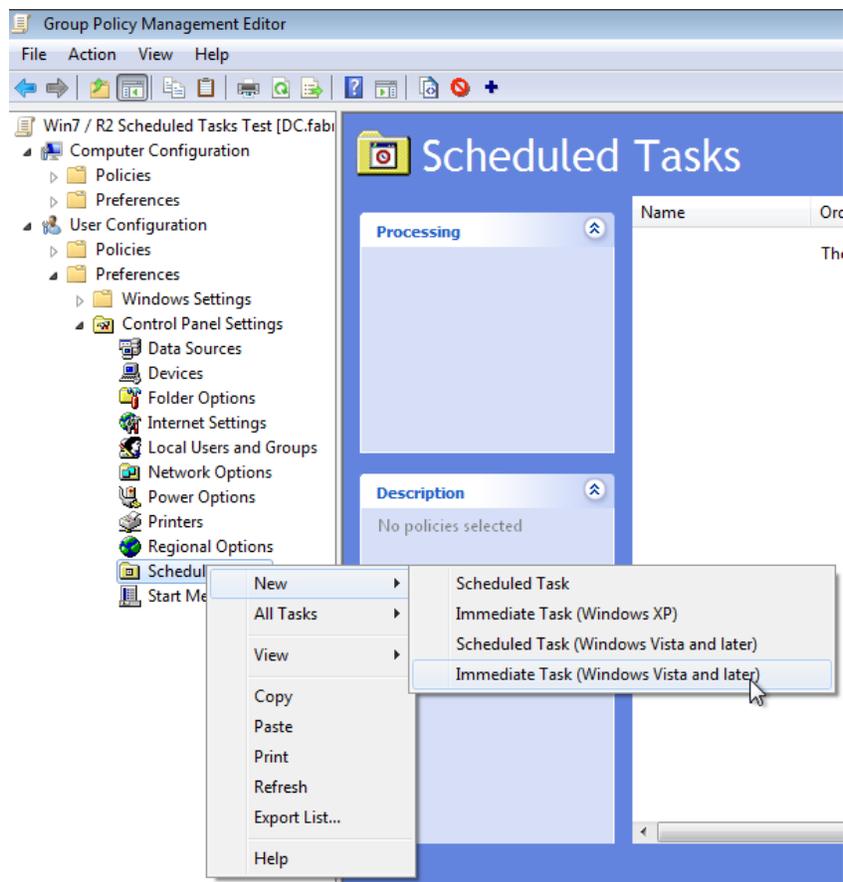


Figure 6. New Immediate Task type

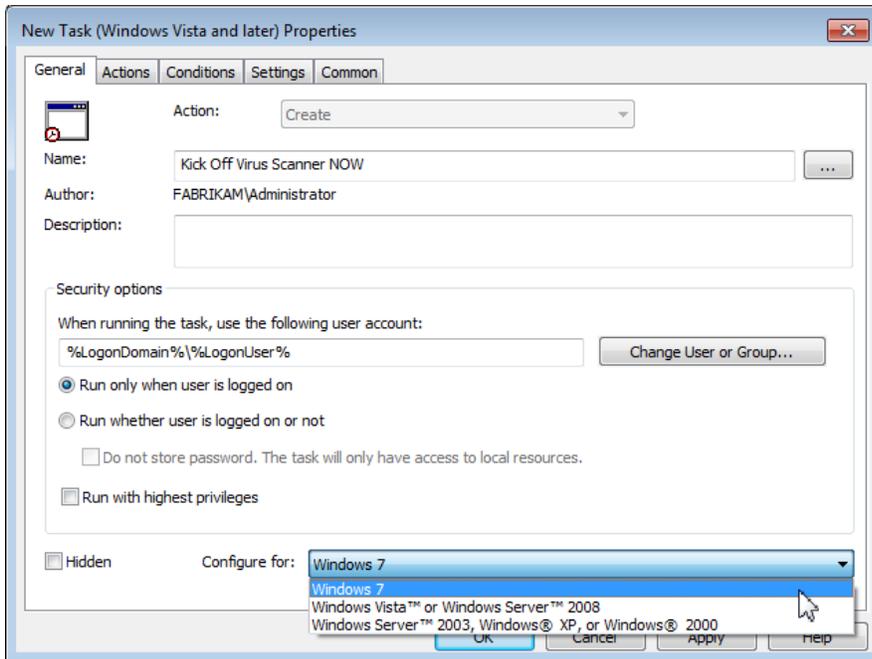


Figure 7. Immediate Task can be configured for Windows 7 (and Windows Server 2008/R2)

However, the bad news is that this “Immediate Tasks” function doesn’t seem to be working in Windows 7 or Windows Server 2008/R2. For this reason, GPOs with the Immediate Tasks item type (for Vista and later) are ignored by the target machine.

Also, it appears that this item type is valid for Windows Vista. However, that is also not true—at least not yet. Similar to the Power Management features described earlier, the Immediate Task type *appears* to be valid for Windows Vista, but as of now (Winter 2009/2010), Windows Vista does not yet have the update ready to process this type of policy setting, as well as the Scheduled Task setting (Windows Vista and later).

However, Windows 7 and Windows Server 2008/R2, do appear to process Scheduled Task (Windows Vista and later) items correctly; again, it’s only the Immediate Task (Windows Vista and later) that is currently inoperative.

The good news is that there’s now a uniform way to assign tasks to all of your machines. Instead of running around from machine to machine, use the power of Group Policy to ensure that consistent, controlled actions are taken based on a central policy.

Tip #5: Use PowerShell to Deploy Scripts

Administrators everywhere are catching PowerShell fever. And for good reason: there are lots of things you might want to do in PowerShell during computer start up or shut down, or at user log on or log off.

Until recently there was no great in-the-box way to deliver PowerShell scripts to target machines. However, Windows 7 and Windows Server 2008/R2 machines can accept PowerShell scripts via Group Policy.

Figure 8 shows the properties of the Logon Properties dialog box found at **User Configuration | Policies | Windows Settings | Scripts (Logon/Logoff)**. Similar settings for the Computer are found in **Computer Configuration | Policies | Windows Settings | Scripts (Startup/Shutdown)**.

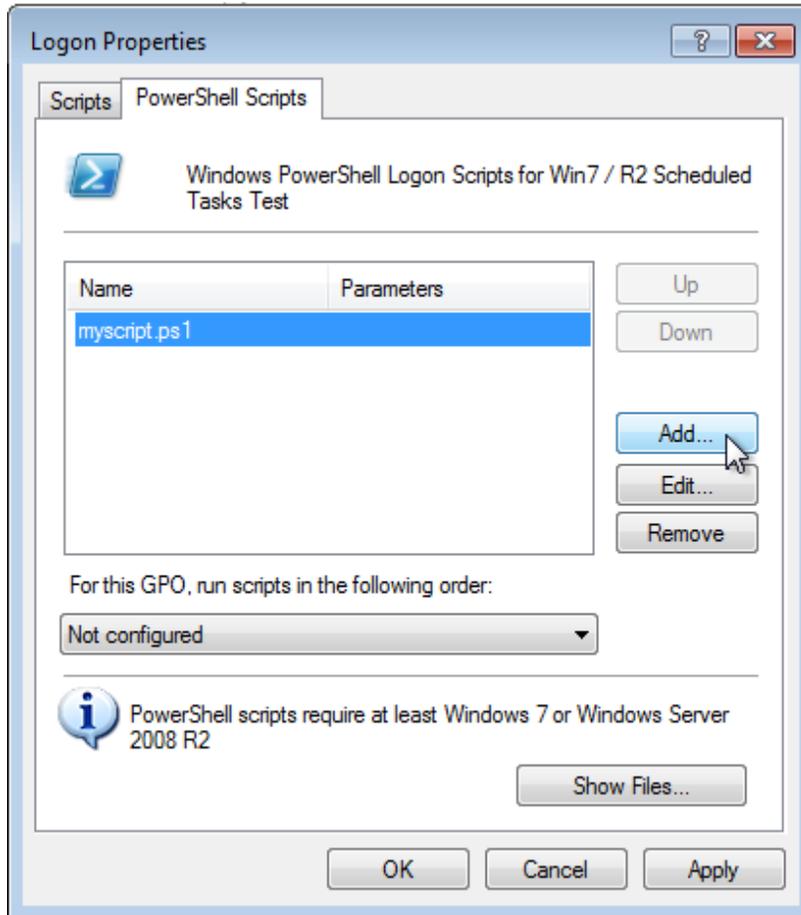


Figure 8. Using Group Policy to deploy PowerShell scripts to Windows 7 clients

However, the pitfall is that anything you do with PowerShell cmdlets exists only as long as the script runs. Therefore, you may get unexpected results. You might think you've mapped a drive letter, only to find that in the outside world, it's not available to users.

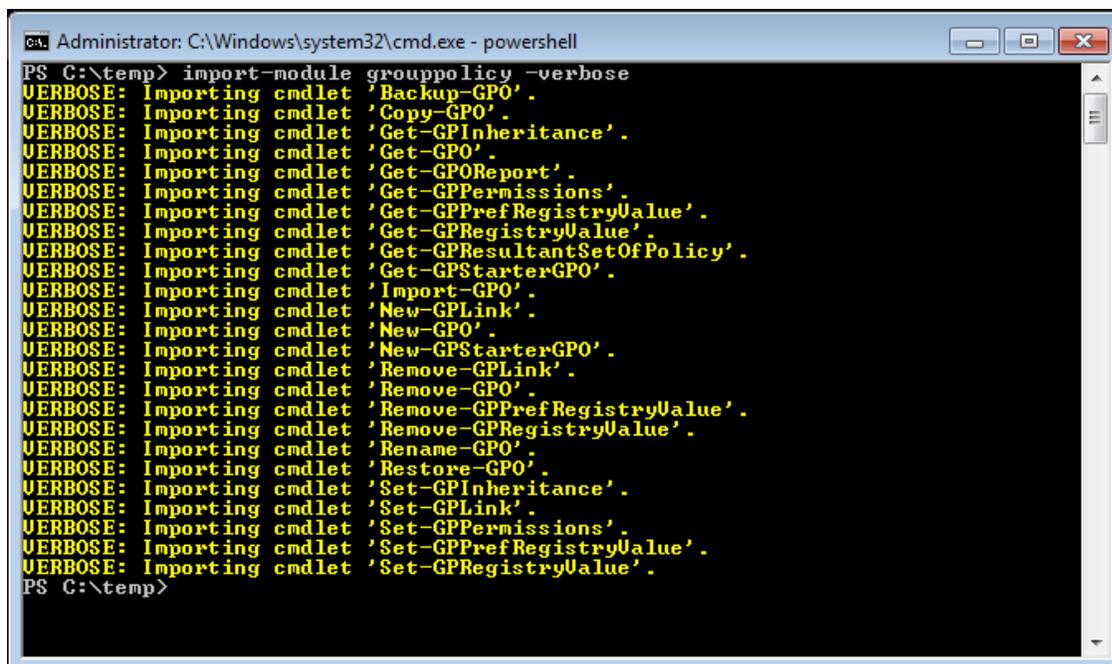
You might want to use PowerShell scripts as a handy way of copying files from the client to the server, rounding up events in the event log and centrally managing them, or for a variety of other reasons. Just remember to output your results to a static location, and don't keep anything important inside the PowerShell bubble.

Tip #6: Use PowerShell for Scripting Group Policy Operations

PowerShell can also be used to script Group Policy operations that are normally only available within the GPMC. For instance, you might want to:

- Create a new GPO
- Restore the settings from an existing GPO
- Link that newly created GPO to an OU

With the new PowerShell support built into Windows 7, you're almost there. To get started on your Windows 7 management machine, start a new PowerShell session. Then type `import-module grouppolicy`. You can optionally tack on `-verbose` to show the cmdlets that the Group Policy PowerShell module can perform. The result is shown in Figure 9:



```
Administrator: C:\Windows\system32\cmd.exe - powershell
PS C:\temp> import-module grouppolicy -verbose
VERBOSE: Importing cmdlet 'Backup-GPO'.
VERBOSE: Importing cmdlet 'Copy-GPO'.
VERBOSE: Importing cmdlet 'Get-GPInheritance'.
VERBOSE: Importing cmdlet 'Get-GPO'.
VERBOSE: Importing cmdlet 'Get-GPOReport'.
VERBOSE: Importing cmdlet 'Get-GPPermissions'.
VERBOSE: Importing cmdlet 'Get-GPPrefRegistryValue'.
VERBOSE: Importing cmdlet 'Get-GPRegistryValue'.
VERBOSE: Importing cmdlet 'Get-GPResultantSetOfPolicy'.
VERBOSE: Importing cmdlet 'Get-GPStarterGPO'.
VERBOSE: Importing cmdlet 'Import-GPO'.
VERBOSE: Importing cmdlet 'New-GPLink'.
VERBOSE: Importing cmdlet 'New-GPO'.
VERBOSE: Importing cmdlet 'New-GPStarterGPO'.
VERBOSE: Importing cmdlet 'Remove-GPLink'.
VERBOSE: Importing cmdlet 'Remove-GPO'.
VERBOSE: Importing cmdlet 'Remove-GPPrefRegistryValue'.
VERBOSE: Importing cmdlet 'Remove-GPRegistryValue'.
VERBOSE: Importing cmdlet 'Rename-GPO'.
VERBOSE: Importing cmdlet 'Restore-GPO'.
VERBOSE: Importing cmdlet 'Set-GPInheritance'.
VERBOSE: Importing cmdlet 'Set-GPLink'.
VERBOSE: Importing cmdlet 'Set-GPPermissions'.
VERBOSE: Importing cmdlet 'Set-GPPrefRegistryValue'.
VERBOSE: Importing cmdlet 'Set-GPRegistryValue'.
PS C:\temp>
```

Figure 9. Importing the Group Policy PowerShell cmdlets

Using the PowerShell console makes it easy to create a GPO from scratch. Just use the `New-GPO` command, as shown below:

```

PS C:\temp> New-GPO -name "A GPO from PowerShell"

DisplayName      : A GPO from PowerShell
DomainName       : fabrikam.com
Owner            : FABRIKAM\Domain Admins
Id               : 4391ff66-197d-4bbe-b83e-4b536a09b543
GpoStatus        : AllSettingsEnabled
Description      :
CreationTime     : 11/17/2009 8:21:33 PM
ModificationTime : 11/17/2009 8:21:33 PM
UserVersion      : AD Version: 0, SysVol Version: 0
ComputerVersion  : AD Version: 0, SysVol Version: 0
WmiFilter        :

PS C:\temp> _

```

Figure 10. Creating a new GPO using PowerShell

Following are some creative things you might want to try when you have a minute.

- To list all the names of the GPOs and when they were created:

```
Get-GPO -all | Select DisplayName, CreationTime
```

- To dump a settings report for every GPO in the domain into separate files:

```

Get-GPO -all | Foreach {
    $report="F:\GPReports\{0}.htm" -f
    $_.displayName.Replace(" ", "")
    Get-GPOReport $_.DisplayName -ReportType HTML -Path $report
}

```

- To back up all GPOs:

```
backup-gpo -All -path \\server\share\gpobackup -comment "Weekly Backup"
```

By using PowerShell to script your Group Policy operations, you can ensure that repetitive tasks there are done correctly every time, without manual labor. But remember that these cmdlets are only available when you're using Windows 7 or Windows Server 2008/R2 as your management machine.

Tip #7: Get Application-level Control Using AppLocker

In tip #3, we restricted undesirable hardware. In this final tip, we'll restrict undesirable software. The Windows default is to allow users to run any application—even single EXE files—without question. But what if that EXE contains something dangerous? Or what if it is an old version of an in-house application that needs to be upgraded?

With Microsoft's AppLocker, you can get close to a world where only the applications you want to run are indeed running.

AppLocker can be found in the Group Policy editor at **Computer Configuration | Policies | Windows Settings | Security Settings | Application Control Policies | AppLocker**.

Microsoft's AppLocker is an evolutionary step from its previous restricting software, Windows XP's Software Restriction Policies. AppLocker raises the bar in several ways.

For instance, you can dictate which software will and will not run via "Publisher rule." Creating the rule is easy: the administrator simply browses to any file by a particular manufacturer (Publisher), and then (provided the file is digitally signed) chooses whether to allow or disallow software based on various criteria.

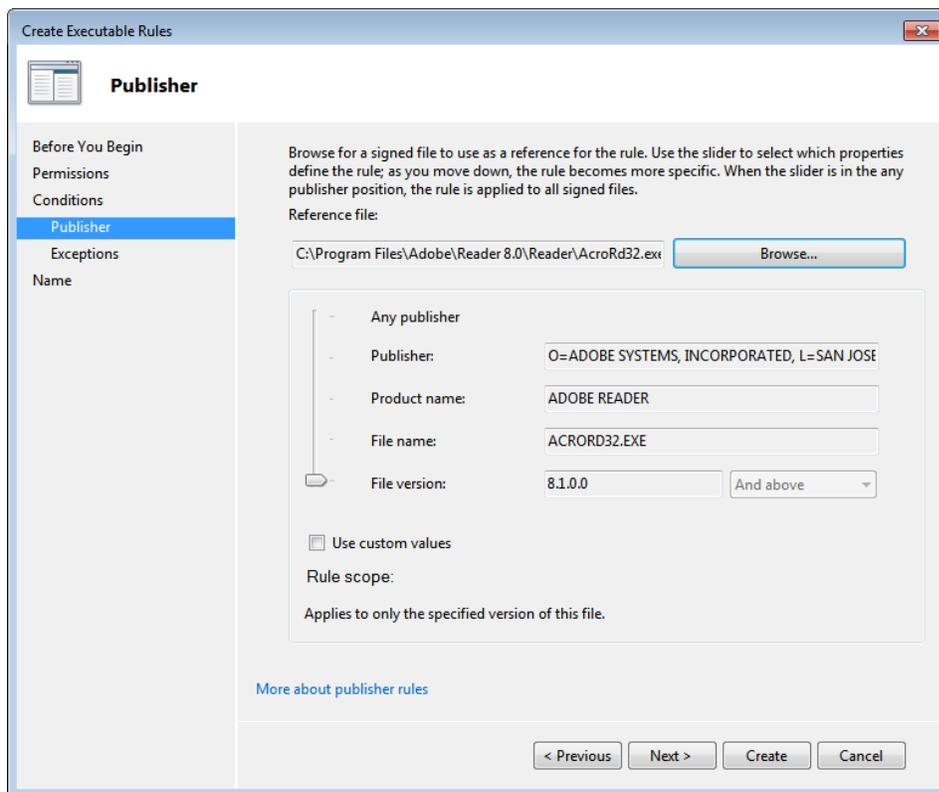


Figure 11. Use AppLocker to restrict or allow software based on rules, such as Publisher rules.

AppLocker can also be used in white-listing mode, which allows only specifically named software to run. If the software isn't on the white list, it's not able to run.

Users who attempt to run prohibited software will see a message like the following:

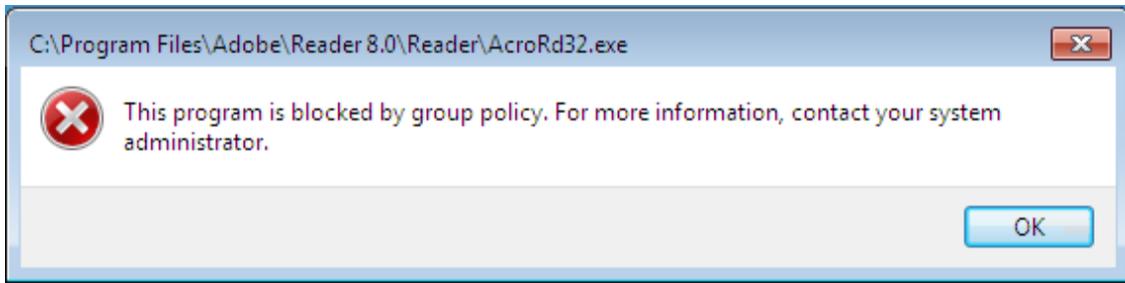


Figure 12. Message from AppLocker to a user attempting to run prohibited software

Again, AppLocker will work only if the target machine is Windows 7 or Windows Server 2008/R2. It is not available for Windows XP; only Software Restriction Policies is available for Windows XP.

Note, however, that even though AppLocker is available for Windows 7, it is not available for all *editions* of Windows 7. Microsoft's documentation (available at <http://tinyurl.com/yjvh34d>) shows that AppLocker is available only for the Enterprise and Ultimate versions of Windows 7; it is not available in the Professional version of Windows 7.

Conclusion

This paper provides a number of ways to strengthen security, automate more tasks, and save money with Windows 7. Because of the power of Windows 7, it is especially important to remember to always test your GPOs in a test environment and ensure they work the way you want before you roll them out into production. You can use a tool like GPOAdmin from Quest Software to create GPOs offline, test them in the test lab, and then roll them into production when you are confident they are working as they should.

To learn more about the topics in this document (Active Directory, Group Policy, and PowerShell) and more, visit the Quest Experts Community at <http://theexpertscommunity.com/>.

To learn more about how to simplify your Group Policy Management and Administration with Quest GPOAdmin, visiting <http://www.quest.com/gpoadmin/>.

About the Author

Jeremy Moskowitz, MCSE, MCSA and Group Policy MVP, is the Chief Propeller-Head for Moskowitz, Inc. and an independent consultant and trainer for Windows technologies. He runs www.GPanswers.com, a community forum for people to get their toughest Group Policy questions answered.



Jeremy can be found speaking at IT conferences and inside corporations all over the world. He has authored or coauthored many books, including his latest two, *Group Policy: Management, Troubleshooting, and Security* (Sybex), and the new *Creating the Secure Managed Desktop: Group Policy, SoftGrid, Microsoft Deployment Toolkit, and Management Tools* (Sybex), both with content available as e-book downloads from GPanswers.com/books.

Since becoming one of the world's first MCSEs, Jeremy has performed Active Directory, Group Policy, and Windows infrastructure planning and implementation for some of the nation's largest organizations. Jeremy frequently contributes to *Windows IT Pro* magazine, *Redmond* magazine, and *TechNet* magazine. Jeremy also teaches Group Policy intensive training and workshop classes recommended by Microsoft. Learn more at www.GPanswers.com/workshop.

About Quest Software, Inc.

Now more than ever, organizations need to work smart and improve efficiency. Quest Software creates and supports smart systems management products—helping our customers solve everyday IT challenges faster and easier. Visit www.quest.com for more information.

Contacting Quest Software

PHONE 800.306.9329 (United States and Canada)

If you are located outside North America, you can find your local office information on our Web site.

E-MAIL sales@quest.com

MAIL Quest Software, Inc.
World Headquarters
5 Polaris Way
Aliso Viejo, CA 92656
USA

WEB SITE www.quest.com

Contacting Quest Support

Quest Support is available to customers who have a trial version of a Quest product or who have purchased a commercial version and have a valid maintenance contract.

Quest Support provides around-the-clock coverage with SupportLink, our Web self-service. Visit SupportLink at <https://support.quest.com>.

SupportLink gives users of Quest Software products the ability to:

- Search Quest's online Knowledgebase
- Download the latest releases, documentation, and patches for Quest products
- Log support cases
- Manage existing support cases

View the Global Support Guide for a detailed explanation of support programs, online services, contact information, and policies and procedures.



5 Polaris Way, Aliso Viejo, CA 92656 | PHONE 800.306.9329 | WEB www.quest.com | E-MAIL sales@quest.com
If you are located outside North America, you can find your local office information on our Web site

© 2010 Quest Software, Inc.
ALL RIGHTS RESERVED.

Quest Software is a registered trademark of Quest Software, Inc. in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.
WPW-GroupPolicy-Main-US-MJ-20100121