



Windows Boston

Group Policy– Group Policy Basics

Published 2007

Clyde G. Johnson, MCSE, A+

What can Group Policy manage

- n Deploy software
- n Security Settings
- n Assign startup/shutdown and logon/logoff scripts
- n Set Standard Security settings for machines
- n Redirect certain folders in user profiles
- n Remote Installation services
- n Software Restrictions

Local Group policy

- n Local Group policy
 - n GPEDIT.MSC
 - n Unique to each machine.
 - n Does NOT need Active Directory.
- n Vista has three layers
 - Administrators
 - Non-Administrators
 - And single users

Active Directory Design

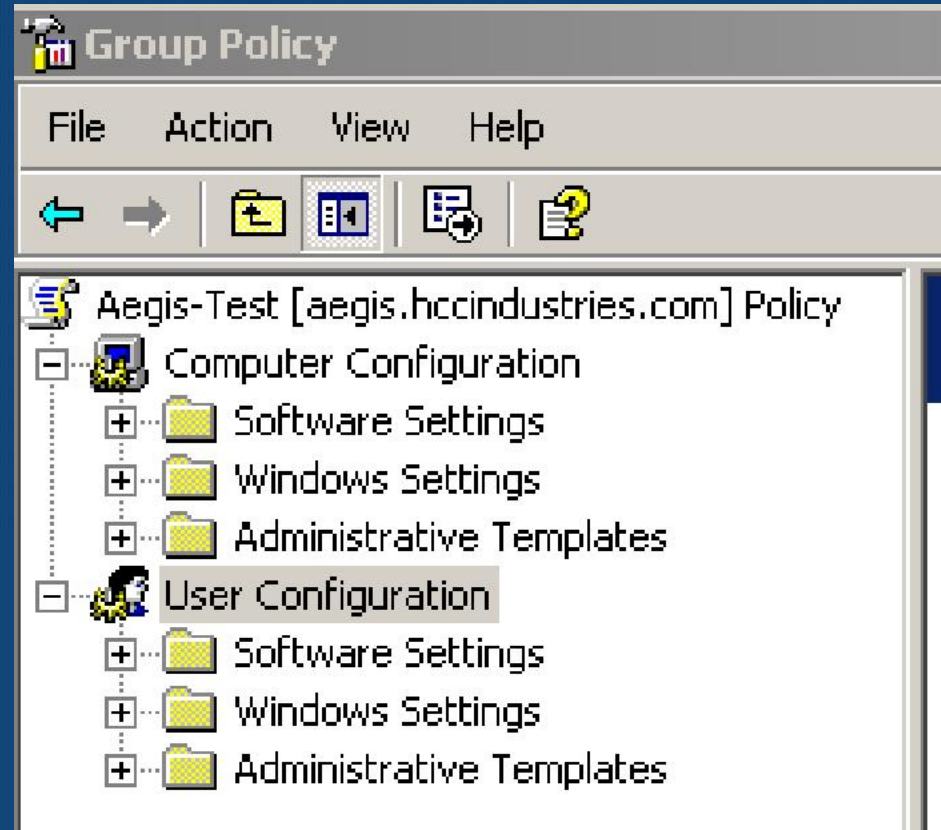
- n Three reasons for an OU
 - n Delegation
 - n Group Policy
- n Example
 - n Windowsboston
 - n Users
 - n Workstations
 - n Servers
 - n Groups

Group Policy Management Console

- n Free update from Microsoft.
- n Installs on Windows XP (with .net 1.1) and Windows 2003.
- n Improved UI and simplified security management.
- n New features
 - n Edit
 - n Copy / Import
 - n Backup / Restore
 - n Report

Group Policy Nodes

- n Two Nodes
 - n User Configuration
 - n Computer Configuration
- n If there are no settings in one node. Then disable the processing of that node.



GPO Categories

- n Administrative Templates (registry settings)
- n Security Settings
- n Software Settings
- n Folder Redirection
- n IE Maintenance

Administrative Templates

- n Collection of registry settings.
- n Are updated with most releases and service pack.
- n Are usually located at %windir%\inf
- n Office has their own.
- n There are 3rd party and custom templates.

When are they applied?

- n Computer startup (computer node)
- n User Logon (user node)
- n User Logoff (user node)
 - n Logoff scripts only
- n Computer shutdown (computer node)
 - n Shutdown scripts only
- n Refresh Cycle (both nodes)
 - n Except folder redirection , software deployment and scripts
 - n This is when machines check for Group policy "changes"

Where to Start

- n Common Desktop Management Scenarios Using GPMC
 - n Set of example policies and a whitepaper
- n Group Policy Settings Reference
 - n <http://www.microsoft.com/downloads/details.aspx?familyid=7821C32F-DA15-438D-8E48-45915CD2BC14&displaylang=en>
 - n Excel spreadsheet with all group policy settings and what OS each setting is supported on.
- n Pick a problem and try to use Group Policy to resolve it.

Common Desktop Management Scenarios

- n Package containing GPOs developed for six different scenarios that can be loaded into AD
- n Includes white paper describing scenarios
- n Excel spreadsheet documenting all GPO settings
- n Scenarios are for the following
 - n Lightly Managed Desktop (e.g. power user)
 - n Mobile User
 - n Multi-User Desktop
 - n AppStation (Highly Managed Desktop) (e.g. admin user)
 - n TaskStation (e.g. single task)
 - n Kiosk (e.g. public workstation)

Read This Book From Cover to Cover

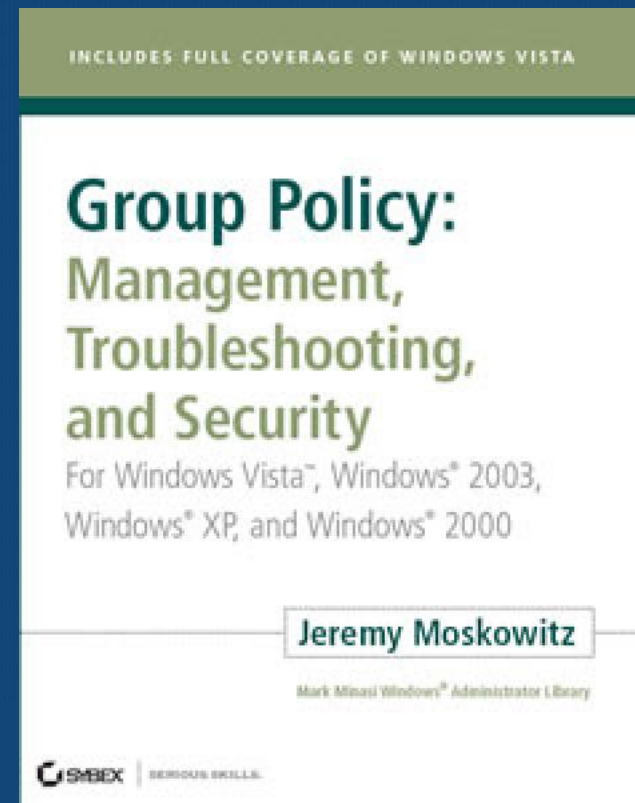
Group Policy: Management, Troubleshooting and Security

For Window Vista, Windows 2003, Windows XP and Windows 2000

By Jeremy Moskowitz

n ISBN 978-0-470-10642-6

n <http://www.moskowitz-inc.com/grouppolicy/book.html>



Testing and Troubleshooting

- n Do not develop on production GPO's
- n Gpupdate
- n GPResult
- n Userenv.log
- n RSOP

Do not develop GPO's in production!

- n TEST, TEST, TEST
- n Group Policy is one of the BEST ways to cause headaches to ALL your users with a touch of a button.
- n Settings are applied to your OU when you click on them. There is NO save button.
- n Create a test environment in a virtual machine. Not on the Network!
- n Don't Change Group Policy settings on production OU's
 - Request a test GPO and use it on test OU.

GPUPDATE

- n Refreshes local and Active Directory-based Group Policy settings, including security settings
- n Use the /force option to reapply all settings even those that have not changed. (usually requires a reboot)

GPRResult /V

- n Use GPRESET to test and track application of group policy
- n GPRESET displays information about a user and computer's domain and group memberships as well as itemizing where all group-policy related settings were applied.
- n This is a very important tool to use when testing a new group policy or attempting to diagnose problems with policies not being applied incorrectly.

Userenv.log

- n Turn on Verbose Logging in the registry.
(KB221833)
- n %systemRoot%\Debug\UserMode
- n When verbose logging is turned on this will log information about the profile and group policy processing.

Problem Solving

- n The greatest use of Group Policy is to solve problems on your machines.
 - n Default mail client
 - n Software rollout
 - n HTML Help
 - n Folder Redirection
 - n Software Restriction

Example: Default mail client

n Problem:

- n Every time Microsoft installed a outlook related patch, This would flip back to outlook. (KB933450).
- n Because Group policy objects were not changed. The "default mail client" group policy was not reapplied automatically.

n Solution

- n Registry setting in a computer startup script.

Example: - Shadowcopy.

- n We decide that we need Shadowcopy.
- n Shadow copy is essentially a previous version of the file or folder at a specific point in time.
- n A snapshot is usually taken twice a day.
- n Relieves the administrator of the burden of restoring files for users. OR makes it easier for the administrator to restore files for users.

Solution : Shadowcopy

- n Acquire a software setup package with an MSI extension.
 - n Extract it.
 - n Create it yourself (win-install)
- n Share and secure Administrative Point
 - n \\servername\share
 - n NTFS Security as a poor man's licensing server.
- n Setup a GPO to deliver the software
 - n Assign or publish the software (assign to computer)

Example : HTML Help

n Problem

- n Microsoft releases a patch that prevent CHM's from being viewed across a network. (896358)
- n These are necessary for our ERP help system
- n Uninstalling the patch is an option. But the vulnerability is real AND being exploited in the wild.

HTML Help Solution

- n Found a registry hack that will let local intranet zone work
- n HKLM\SOFTWARE\Microsoft\HTMLHelp\1.x\HHRestrictions\MaxAllowedZone=1
- n But this is not exposed in any Group Policy now existent.
- n We created a custom group policy template and applied it to all the workstations.

Example: Folder Redirection

n Problem:

- n People have documents on their desktops.
- n Not backed up or encrypted.

n Solution:

- n Create a policy that redirects their "My documents" and "Desktop" folder to the network.
- n For laptops we created a policy that enables offline folders AND encrypts the local folder they are in.

Example. - Software restriction

- n Requested to deny the use of solitaire.
- n We don't load it by default.
- n Used software restriction policy.
 - n This is a very dangerous thing.
 - n It's deny everything by default.
- n Disabled Solitaire by Hash rule.
 - n This means that no matter where or by what name solitaire goes by. It is restricted.

Vista

- n Overhaul of the ADM templates (ADMx)
 - n administrative template files in Vista use a new XML-based file format (.ADMX).
- n ADMx Central store
- n +800 new or expanded Policies (now over 2k)
- n Control removable media
- n Control power management

Resources

- n [How To Delegate the Unlock Account Right](http://support.microsoft.com/kb/294952)
<http://support.microsoft.com/kb/294952>
- n [Group Policy Management Console \(GPMC\)](http://www.microsoft.com/windowsserver2003/gpmc/default.mspx)
<http://www.microsoft.com/windowsserver2003/gpmc/default.mspx>
- n [Introduction to Shadow Copies of Shared Folders](http://www.microsoft.com/windowsserver2003/techinfo/overview/scr.mspx)
<http://www.microsoft.com/windowsserver2003/techinfo/overview/scr.mspx>
- n <http://www.appdeploy.com/>
- n [Using Administrative Template Files with Registry-Based Group Policy](http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/management/gp/admtgp.mspx)
<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/management/gp/admtgp.mspx>
- n [How To Use Software Restriction Policies in Windows Server 2003](http://support.microsoft.com/kb/324036)
<http://support.microsoft.com/kb/324036>
- n [Using Software Restriction Policies to Protect Against Unauthorized Software](http://technet.microsoft.com/en-us/library/28df04f8-f97f-7143-9536-5ca33b55d1a9.aspx)
<http://technet.microsoft.com/en-us/library/28df04f8-f97f-7143-9536-5ca33b55d1a9.aspx>

Resources (cont.)

n Userenv and GPE logging

http://searchwinit.techtarget.com/tip/0,289483,sid1_gci1250007,00.html

n Debugging GPO problems with Userenv logs

http://searchwinit.techtarget.com/tip/0,289483,sid1_gci1249039,00.html

n <http://www.gpoguy.com/FAQs/troublefaq.htm>

<http://www.gpoguy.com/FAQs/troublefaq.htm>

n Group Policy Common Scenarios Using GPMC

<http://www.microsoft.com/downloads/details.aspx?familyid=354b9f45-8aa6-4775-9208-c681a7043292&displaylang=en#Overview>