Master Windows 2003 Group Policies

By Guy Thomas (Revised November 2005)

Table of Contents – (Use Find to locate headings)

Who is this Group Policy ebook for?

Administrators who want a detailed view of Windows 2003 Group Policy settings.

Experienced network managers who wish to lockdown their users' Start menu.

Network Architects who need to turn a desktop vision into reality.

Those upgrading from Windows 9x or NT 4 to XP.

What are Windows 2003 Group Policies?

If you wish, Group Policies can control every aspect of a computer desktop. While the plan is to control the configuration of both the user and the computer settings; the technique is to define each setting once in active directory. For example, if you need to change everyone's proxy server, then add the IP addresses to a group policy rather than edit every Internet Explorer manually.

It may help to remember that Group Policies manipulate registry values, so if the item that you want to control is in the registry, then it can be set by a policy. Where registry keys do not have ready-made policies, it is possible to create your own policy templates. However, designing your own templates would be a specialist job for your developers.

Some say there are 700+ built-in polices for XP, while others tell me that there are over 850. What ever the exact total, the point is that group policies are here to stay, and that each new version of Windows will bring yet more settings to organize the desktop.

Here are the commonest policy categories for XP / Windows Server 2003.

Security settings, passwords: length, frequency, lockout duration.
Desktop settings, which icons appear, and which are features are hidden.
Software assigned to the user, which programs are available from the start menu.
Folder redirection, where is the 'My documents' are stored?
Settings which dictate the operating system behaviour, for example, disable unnecessary services.

Guy's Group Policy Mission

My mission is to bring each group policy category or folder to life. I want to save you time by concentrating on what I consider are the best settings in each group policy folder. Look out for 'Guy's top selections' on each page. Occasionally, I express an opinion that a policy is of limited use - no sitting on the fence! However, even if a policy is only needed for specialist configurations, I still point out its purpose, just in case it applies to your situation.

Before you begin evaluating policies, I urge you to decide on the security rating of your organization. It is important to have a reference point; otherwise it will be difficult to gain a perspective of what makes sense for your users. My advice is aimed at those who need medium security setting for their domains; therefore, if you are a high or low security company then make the necessary adjustments when assessing my selections.

Remember, that the more security that you enforce, the more work there will be for you. For instance, do not insist on a 14 letter, complex password, just because they are the highest settings. However, if there is a good business case for this level of security, then fair enough, but does take on extra help desk staff to cope with the resultant password lockouts.

Pre-requisites for creating policies

- The advice and screen shots in this section are designed for Windows Server 2003, however many of the settings are available in Windows 2000.
- Group Policy Management Console is installed
- You create a test OU. (Not essential, but safer than using the default domain policy)
- Right click your OU, Properties, Group Policy. Click on Open.
- Right click on your OU, and select 'Create and Link a GPO Here..'
- Right click your policy, then edit.

Next step

If you are itching to start configuring group policies, the best place to begin is here at User Configuration

Group Policy Overview

Each new operating system brings with it a paradox. On the one hand the new version is meant to be easier, while on the other hand it brings more features to master, more sub menus to explore and more settings to configure. When I apply this paradox to Group Policies, my conclusion is this: Windows 2003 produces a significantly better managed desktop than NT and W2K, however Group Policies are more difficult to master because there are more features, components and settings.

Topics for Group Policy in Windows Server 2003.

The Big Picture

The concept behind Group Policies is that administrators configure settings once, and then the settings apply continuously to the users. Furthermore, Group Policy can be applied to computers, so that you can control the settings no matter who logs on.

The old saying 'Prevention is better than cure', definitely applies to Group Policies. A good Group Policy will give greater productivity for the users, and reduce your time fixing silly problems. Think of all the damage and time wasting caused by users fiddling with control panel settings. I once saw a user set the screen refresh rate faster than the monitor hardware would support, his screen literally went up in smoke! If only the administrator had set a group policy that disabled the Display Tab and thus prevented an expensive blown monitor.

Group Policy - Strategy

Just wading through the 100's of Policies is a Herculean task. My suggestion is that you commission two opposite approaches. Firstly, ask a 'Techie' who understands Windows 2003 to go through the policies and select those settings that he thinks appropriate. Secondly, invite a manager to produce a vision, or wish list of what he believes a user's desktop should look like. Finally, bring the two disparate mind sets together and weld them into your Group Policy.

One neglected aspect of group policy is positive thinking. Administrators become obsessed with screwing down the desktop and ignore settings which could help the users. Take the previous example, many people discover that the default refresh rate of 60 Hz literally gives them a headache; the administrator should have been pro-active and created a policy that set the refresh rate to 80 Hz.

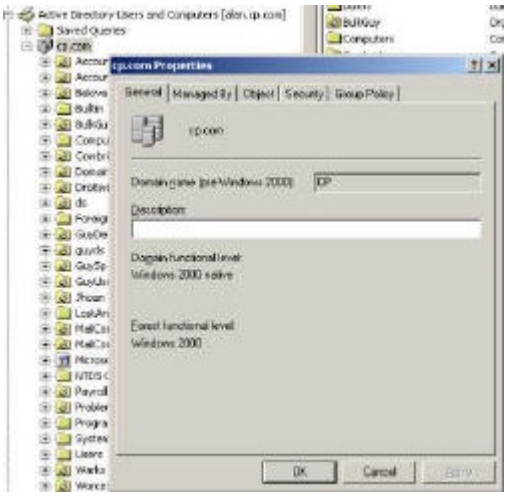
Everyone loves deploying Group Policies. To do the job justice you need at least 15 man-days even for a smallish domain. I say man-days because it is better to have a team of 2/3 than leave it all to one individual.

Assigning Software

Make your mantra: 'If there is a business case for an application, then create a Policy which delivers that package to the Start Menu.' Techies like this approach because they can apply service packs and upgrades from one central place, and no longer need to visit each desktop to upgrade a program. Such polices operate from the Software Settings folder. If you want everyone who logs on to use an application, then Assign it

to a computer; however if the user needs special software wherever they logon, Assign it at the User Configuration folder. If you are undecided, favour the Assigning to Users rather than Computers.

Getting Started - Create a Group Policy



This is how you begin with Group Policies. Navigate to the Active Directory Users and Computers. Right click the Domain object, Properties, Group Policy (Tab) now 'click' the edit (button) and you will see the policy settings.

A less risky method of easing your way into Group Policies would be to create a test OU, and then make a brand new policy.

Group Policy Inheritance for Windows Server 2003

This page introduces the objects and techniques that you need to create the best Group Policies for your active directory. In particular, this page shows you how to get the most out of your policies by judicious use of 'Enforce' and 'Block Inheritance'.

Group Policy Container

Group Policy objects have to be created and held in a container. This container could be at the domain, OU or site level. Do remember that Windows 2003 comes with the Domain Group Policy and the Domain Controller Group Policy. At some stage in their career everyone forgets that the domain level is the one and only level that you can set domain account policies, for example password length, lockout duration. It is also easy to overlook the Domain Controller Group policy when you are configuring local settings for those servers.

A good reason to create more policies is because you want each department to experience independent desktop settings. The container for these diverse policies is the OU (organizational unit). It is also possible to set policies at the site level, but I would discourage this except for the largest companies. My reasoning is that troubleshooting policies in two locations is challenging enough, so you do not need the extra difficulties caused by a policy at the site level which you had forgotten about. Moreover, setting policies at the site level would affect the entire domain in that site.

Summary, make the domain and OU objects your vehicles for group policies. If possible, avoid using Site or Local Group policies.

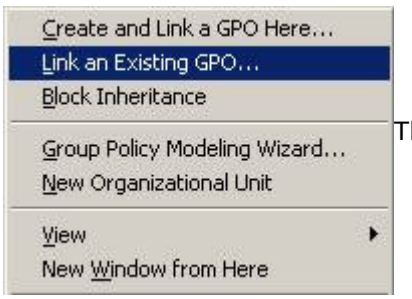
Creating group policy objects (GPO).

Just to be clear on the semantics, the settings that I discuss in the following pages are held in Group Policy Objects (GPOs). These policies are created in, or linked to, the container objects at the Site, domain or OU level.

To create your GPO, right click the OU, select Properties, and then click on the Group Policy Tab. (See Diagram)

Next click 'Open' and choose your OU and select: Create and Link a GPO here. Now you are ready to edit the Group Policy settings and thus fashion the desktop of your vision.

Group Policy Links



Another option is to Link an Existing GPO. Otherwise known as : 'The one I made earlier'. This concept involves recycling policies that you designed for other OUs. Apart from not re-inventing the wheel, the benefit is that the links themselves have permissions.

Group Policy Inheritance

Mostly you need not worry about group policy inheritance, because if there is no conflict, then there is no problem. If 'Remove Run Command' is enabled at the domain level, and 'Add Logoff to start menu' is enabled at the OU, there is no fight for control. It is only when 'Add Logoff' is **disabled** at the OU then we have a conflict with 'Add Logoff **enabled** at the domain GPO.

Group Policy Inheritance

(Local Policy XP and Member Servers)
Site
Domain
OU
Child OU.

Enforced (Also known as No-Override)

Surprisingly, by default, the settings at the lowest level win. What ever is set at the child OU will override the same policy setting at the domain level. If you are thinking, 'That cannot be right; that is not what I intended', then I have just the option for you: 'Enforced'. If enforced is set on a GPO at a higher level then the child objects and the sub, sub OUs cannot override that policy.

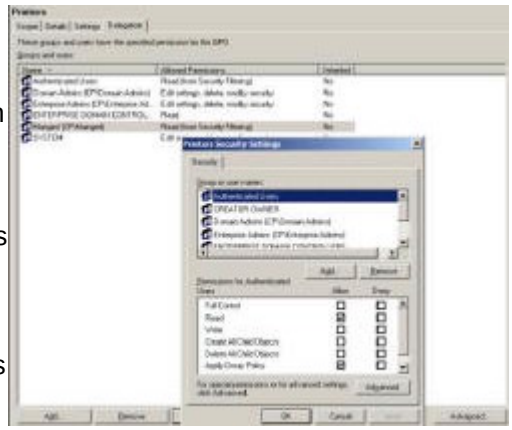
Block Inheritance

There is one more setting that you should know about and that is Block Inheritance. This is what I call the anarchists setting. If you allow delegation at the OU, level then it is possible to stop any policies coming down from the domain. However any policies that have been 'Enforced', cannot be blocked.

Remember that block inheritance affects the whole OU, not just one policy.

Group Policy Security - 'Filtering'

As you design your policies, keep in mind for whom they are intended. For instance, is a policy needed for all users or just for one department? Microsoft calls controlling who gets particular settings as 'Policy Filtering', Guy calls it adjusting the security tab.



When you are new to group policies it is tempting to experiment with viscous settings to lockdown the user. The problem arises, if you apply a high security policy at the domain level, and then you forget that affects even the administrator. You only shoot yourself in the foot once, thereafter, you remember to filter the policy so that only the intended users get your vicious settings.

There are two philosophies for filtering policies, either rip out the Authenticated users and just add the group you have in mind for that policy; alternatively, deny the policy to Administrators, so they will not be 'under the thumb' of an aggressive lockdown policy. If you wish to edit permissions, navigate to the menu above. Note the Delegation tab and in particular the Advanced button on the bottom right.

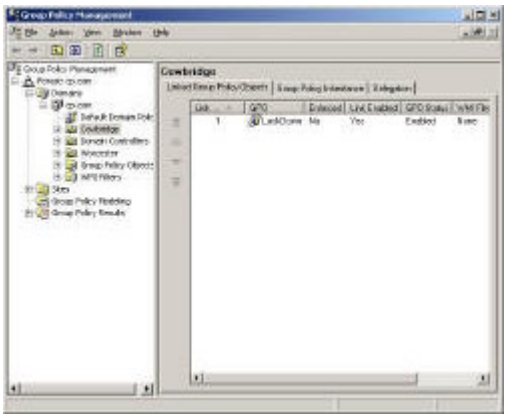
Group Policy Creator Owners

What's new with delegation of permissions? In Windows 2003 there is a new built-in global group called Group Policy Creator Owners. My own view is that I would confine configuring Group policies to a small select group of experts and not allow delegation of Group Policies to people in each OU. My point is that while I am usually all for delegation, creating users - yes, reset passwords - excellent use of delegation, but in the case of delegate Group Policies - no. Leave Group Policies to your top administrator team.

Group Policy Management Console (GPMC)

Microsoft provide a rich source of tools for managing Group Policy. The GPMC is one of THE best new features in all of Windows Server 2003.

Group Policy Management Console (GPMC)



Firstly, the GPMC is designed for Windows Server 2003 rather than W2K. Download the GPMC add-on from Microsoft's site. It is well worth the effort in installing to gain the extra setting to manage your Group Policies.

It seems that GPMC will work on Windows 2000 Domains. (However, I have not got it to run yet!)

The Group Policy Management Console (GPMC) unifies Group Policy management across your active directory forest. Before GPMC, administrators needed the following tools to manage Group Policy; the Microsoft Active Directory Users and Computers, the Delegation Wizard, and the ACL Editor. Not only does the GPMC integrate the existing Group Policy tools, but it also brings these exciting new capabilities:

A user interface that makes it easier to use and manage Group Policy.
New WMI filtering means that you can apply policies to a particular machine, or Assign software only if there is enough disk space.
Backup, restore, import, and copy Group Policy Objects (GPOs).
Simplified management of Group Policy-related security.
Reporting for GPO settings and Resultant Set of Policy (RSoP) data.
Programmatic access to the above GPO operations. Note that it is not possible to programmatically set individual policy settings within a GPO.

RSoP Snap-in (Resultant Set of Policy)

Microsoft provide a snap-in called RSoP for showing a given combination of policy settings. I find that if you install the GPMC, then you do not need this RSoP. However, if you do need the RSoP it is intuitive to use and comes in two modes:

Logging mode. In logging mode, the RSoP snap-in tracks the policies that you apply. In this mode, the tool shows the actual policies for a given user or computer.

Planning mode. In planning mode, the snap-in indicates the set of policies that *would be* applied if you deployed the policy. You can perform what-if analyses on the user and computer; the domain, and organizational unit.

Gpupdate

I am so pleased that Windows 2000's Secedit has been superseded by Gpupdate on XP, the old Secedit syntax was horrendous. Mostly, I just run Gpupdate in a 'Dos Box', on its own, occasionally, I append the following switches:

/target:computer or /target:user applies only to the user or computer section of your policy. Normally I would use plain Gpupdate without the optional target switch.

/logoff Useful for settings that do not apply until the user logs on again.

/boot Handy for configurations which need the computer to restart.

/force reapplies all settings.

Gpresult

While I prefer the GPMC console above, here is a handy command line utility to display the results of group policy. What I particularly like is the /user switch. Take the example where you are logged on as the administrator, but wish to test a user called Psycho's settings. Rather than logoff then logon as that user, just type: gpresult /USER psycho. Do remember the /USER. This would be a mistake gpresult /psycho.

Dcgpofix

This handy command line utility restores the default Group Policy objects to their original state. You find your 'get out of jail card' = Dcpgofix in the \windows\repair folder.

Syntax and Switches

dcgpofix [/ignoreschema][/target: {domain | dc | both}]

Example: dcgpofix /target: GuyDom

Caution

This tool will restore the default domain policy and also the default domain controllers' policy to their state just after installation. Naturally, when you run dcgpofix, you lose all changes made to these Group Policies.

By specifying the /ignoreschema parameter, you can enable Dcgpofix.exe to work with different versions of Active Directory. However, default policy objects might not be

restored to their original state. To ensure compatibility, use the version of Dcgpofix.exe that is installed with the operating system.

Group Policy Results and Modeling for Windows Server 2003

Group Policy Results is one of THE best new features of Windows Server 2003. It allows you to see at a glance all the policies and all the settings that will apply to a user when they logon at a named machine. Close behind comes Group Policy Modeling; take the time to run the Wizards through their paces and to check the numerous tabs and buttons.

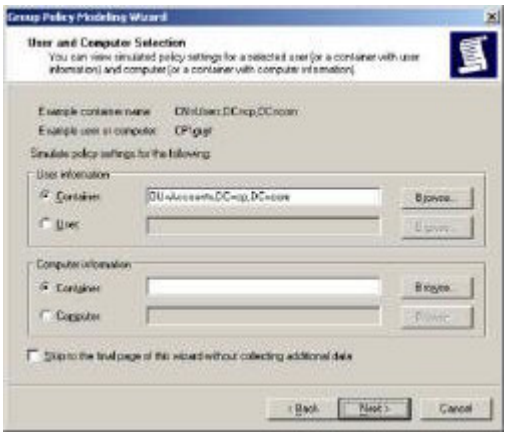
Group Policy Results

In a nutshell, Group Policy Results saves you time. No more logging off, then logging on as the user that wishes to check.

As with so many configurations, a wizard guides you through the choices of which user at which computer. Do not neglect the Settings tab because it will show you details of the configurations enabled or disabled within the policy.

It may be churlish to criticise, but one problem is that the users need to have logged on once at the computer before you can create a report.

Group Policy Modeling



It is almost as though Microsoft have read my mind when I criticised the Report Wizard and provide a Modelling Wizard where you can choose any OU and play 'What if' games with the policies.

As with the reports, the Modelling Wizard saves the settings so that you can quickly and easily refer to the different settings, just click on the show and hide hot links. Once again, take the time to explore all the menus, otherwise you will not appreciate the power and scope of these tools.

(As an aside, modeling really is spelt with one 'L', possibly an American spelling?)

10 Tactics for your battle with Group Policies

1) The most important tactic is stunningly simple. Create your policies **before** you roll out your (XP) clients. So many companies introduce wonderful group polices months after the new desktop roll-out. Instead of amazing their users with the excellence of their policies, all they get is resentment because people are suddenly denied features they like and have become accustomed to.

'Barking' Eddie convinced one group of users that their company that had bought a special edition of XP, and that's why there were so few settings. You and I know that it was just group policies applied cunningly to a regular edition of XP.

2) Create a test OU. Make this trial Organizational Unit your focus for group policy experiments. Naturally, create test users and a test computer and make sure they are in the OU you where you trial your policies.

3) Favour one policy with lots of settings. Avoid zillions of policies each with one setting. At the very most a user should be the subject of more than a handful of policies, otherwise troubleshooting becomes complex.

4) Be on the lookout for positive group policies, from the simple 'Enable Logoff' to the pre-configured proxy settings and 'Pre-Populate printer locations'. My message is keep your eye out for policies which will improve your user's experience and save them time.

5) Assign Software rather than Publish. No-one is going to find your lovely programs by going to the Add or Remove Programs. The other benefit is that assigning software uses elevated rights for the installation.

6) The 'Enforce' and 'Block Inheritance' are excellent tools for troubleshooting, but only use them sparingly in the production network.

7) Make it your reflex to amend the Security tab so that Administrators are set to: Deny - Apply Policy. The risk is that you will 'shoot yourself in the foot' with a really vicious policy, for example, deny the right to logon locally. Just in case of a problem, create a full administrator in special OU where you block inheritance and never apply any policies.

8) Surround yourself with the best tools. GPMC, Gpupdate and also the Report and Modeling Wizard.

9) If you are serious about group policies, document the settings. An Excel spreadsheet would be an ideal vehicle to hold all the information.

10) Favour the user settings rather than the computer policy settings. Where there is a 50: 50 decision to apply a policy setting to a computer or a user, then favour the user configuration. The other benefit is that you tend to keep all the policies in one area and so make troubleshooting easier.

Troubleshooting Group Policy

My best advice for troubleshooting is this: Put yourself in the right frame of mind. Get into 'State' as Anthony Robbins would say. Believe that you are going to solve this problem.

80% of all problems are caused by a simple fault. In the case of Group Policies, check that the user or computer is in the OU that you are testing. By default, all computers are in the Computer folder. That means that if you set a policy at an OU, the computer settings will have no effect on any computers still in the original computers folder. A variation of this problem is, that people do not realize that their Domain Controllers have their own special policy, again find the Domain Controller container and configure that default policy. I would not advise moving the Domain Controllers into an OU.

So, if you logon as user and none of your policy settings apply - check to see that the user account is in the same OU as the policy you are testing. Incidentally, this is why I always include one or two trivial setting along with main setting that I am testing. If the trivial settings work, but the one I am testing fails, then that pin points where the fault lies.

Now for more specific and practical advice:

See Next page……

	Ask your self what was the last thing I did? Now undo those settings and see if that cures your problem
Q1) Why is my group policy not working?	Check Block Inheritance. Possibly a No Override policy is preventing your settings. Has the user 'Apply Policy' Permission? Is the user and computer in the correct OU?
Q2) You want to know which Policies are in force	GPMC - Run the results Wizard RSoP - Useful for Windows 2000 Gpresult - Improved Switch /user
Q3) Can I refresh the policy without a reboot?	That depends! Most do. Gpupdate refreshes the policy instantly; however some policies require a reboot or a user to logon again. For example Software policies.
Q4) Why can't I open the policy editor?	Perhaps you only have read only permission. Full control is needed to open the GPO.
Q5) What causes 'Failed to open the Group Policy object'	Most likely a DNS problem. Try NSLookup, Ping, Ipconfig to confirm or deny the diagnosis.
Q6 Why do I get the 'Missing Active Directory Container' message?	Hopefully, its just a DC replication delay. Try and force domain replication in Active Directory Sites and Services, drill down trough Server to NTDS and synchronise.
Q7) How can I stop this error: 'The Feature you are trying to install cannot be found'?	Check the share and NTFS permission on the .MSI package folder.
Q8) I have made a terrible foul up. My policies are a disaster.	Run DcGPOfix to return the default group policies to their original state.
Q9) My Script Policy does not work	For specific help with logon scripts, check out the Scripts section.
Q10) Where do I start creating a Group Policy?	Navigate to the Active Directory Users and Computers. Right click the Domain object, Properties, Group Policy (Tab) Next 'click' the Edit (button) and you will see the policy settings.
If all else fails	Check the Event Viewer. Filter the Application Log for Source = SceCli. Really we should have checked here FIRST! If you find a suspicious entry, then check the ID numbers and details in TechNet.

WMI Filters for Group Policies

WMI Filters allow you to select only computers that meet your chosen criteria. Naturally, your Group Policy will only apply to the objects that match your filter. For example, you want to assign an .MSI package, however you are worried that disks on the XP workstations are full. The answer is to design and build a WMI filter.

WMI Filter Topics

WMI Filter - Example 1

Below is a WMI filter which checks the free disk space on the C: and D: drives.

SELECT * FROM Win32_LogicalDisk WHERE (Name = " C:" OR Name = " D:") AND DriveType = 3 AND FreeSpace > 20000000 AND FileSystem = " NTFS"

Note 1: DriveType value = 3 means a local disk
Note 2: 20000000 = 20MB.
Note 3: Your Keyword - Win32_LogicalDisk

WMI Filter - Example 2

Here the WMI filter checks that the Operating System Name is XP.

Select * from Win32_OperatingSystem where Caption = " Microsoft Windows XP Professional"

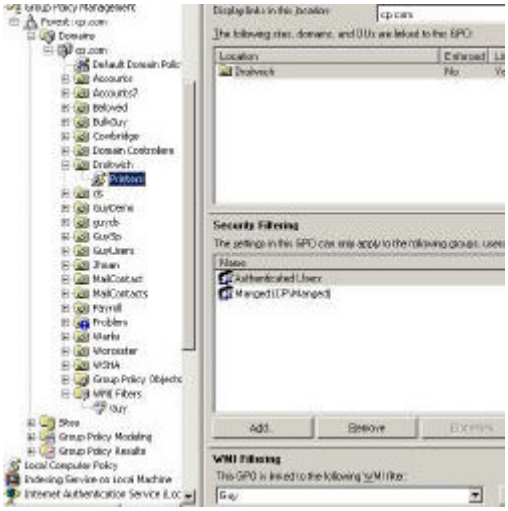
Note 1: The Keyword is Win32_OperatingSystem

In truth you need to be a minor expert on WMI interface to create your own WMI filters from scratch. However, the built-in utility WBEMTEST is a great teacher.

Other ideas for filters

- Hardware - Pentium II or later
- Service packs - SP1 or later
- DHCP - Service
- Fancy filters e.g. Registry settings or even event log ID

Where to apply WMI filters.



Once again, use the GPMC to create and apply your filters. The WMI filters have their own folder where you design and build the queries.

Then you link the filter to the appropriate group policy via the drop down box on the very bottom right of the diagram.

How the filters work

A WMI filter consists a query that is checked against the WMI data on the target machine, the answer is always true or false. Technically, the WMI filter is a separate object from the GPO in the directory. To apply a WMI filter to a GPO, you link the filter to the GPO. This is shown in the WMI filtering section on the Scope tab of a GPO. Each GPO can have only one WMI filter; however the same WMI filter can be linked to multiple GPOs.

Note that these WMI filters only work on Windows XP and later operating systems. Windows 2000 and earlier clients just ignore any WMI filter and the GPO is always applied to all objects. In effect it means that for these old clients the WMI filter is always true so there is no filtering.

Summary

Here is a great idea to fine tune your Group Policy and only apply the settings where there is sufficient disk space. WMI filters are limited only be your imagination, or your knowledge of WMEMTEST.

XP SP2 - Even More Group Policies

XP SP2 has introduced a whole lot more Group Policies. It reminded me that if you have the patience and a third-party tool, then you too could create a Group Policy for virtually any setting in the Registry.

Mission to add the new policies (.adm) to Windows Server 2003.

This was one the strangest missions that I have ever undertaken. The concept was mind blowing, but the practical easy.

The concept is to Upgrade, stress Upgrade, existing Group Policy Objects.

Logon to an XP machine that is part of the Windows Server 2003 domain.

Make sure that SP2 has been installed on this XP machine.

Get the Windows Server 2003 Administrative tools on this machine.

Start (Button), Run \\server\admin$ system32, adminpak.msi.

Use the Active Directory Users and Computer to edit your existing Group Policies. If you are still with me, then you will be doing this from the XP machine.

The act of editing miraculously updates the .adm files on the server. Strange but true.

Whilst I was sceptical, the above method worked a treat for me.

Order of Group Policy Folders

The order of Group Policies is a mystery. The folders are certainly not listed alphabetically, what I have decided to do is keep the same order as you see in the Group Policy interface.

Software Installation

Assigning software via group policies is one of THE great ideas in computing. The intention is to pamper the users by providing all the programs that they need for their job. Not just MS Office, but any program with an .MSI extension can be installed using this technology.

You have to decide between two strategies; assign the software the user, so they receive the software no matter where they logon. Alternatively, assign the software to the computer, with the result that everyone who logs on gets that .msi package. If the decision is close, then I would favour the User Configuration.

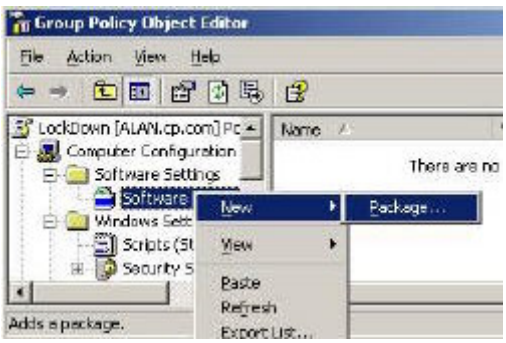
Topics

Getting Started - Assign your .MSI package

Configuring Software Installation has a different 'look and feel' from other group policy settings. What you find with Software policies is that there are new menus and a different logic.

You may have noticed that modern software arrives as an .MSI package. All you need to do is prepare the server is simply share out the folder from where you are going to roll-out the package.

Back at your GPO, all you need to do is right click on the Software Installation box and select, New, Package.



Trap 1: You type in a local path, for example e:\ software. This is incorrect - watch out for the warning message. What you rally need is a UNC path, for example \\ server \share.

To avoid this trap, I type \\ server in the browse box, then select the share containing my .MSI file.

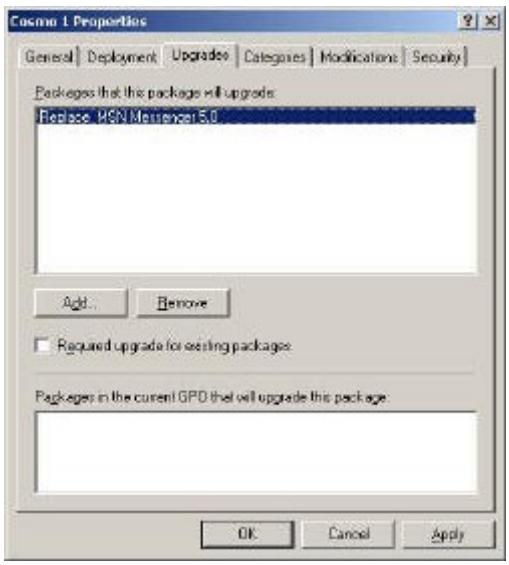
Product life-cycle

Designing a Software Installation Policy is a great example of investing time up front, which later repays with interest. When you are installing new software, the fact that one day it will be obsolete, is not at the forefront of your mind. Service packs and upgrades are not a concern - yet.

Remember that the biggest benefit of assigning software through group policies, comes later when you need to upgrade or removal the original program. No need to visit those irksome users, all you have to do is click a few boxes and the original software package can be replaced.

Deployment

There are useful options for fine tuning your deployment strategy. I particularly like the ability to remove the application when the user moves out of scope; for instance, if they get a promotion and move to a different OU.



Upgrading

Firstly obtain the updated .MSI package. Then add the .MSI to the group policies, apply the same method as when you assigned the original package.

You are now ready to replace the original package with the newer .MSI.

Trap 2: Be careful where you right click and select properties. The blue and white box called 'Software Installation' has properties; in addition, each .MSI package has its own properties. Here you need to select the Package (Not 'Software Installation')

Removing Packages

A rare event. If you simply click on a package and then hit the delete key, nothing happens. The trick is to right click, select 'All Tasks' and then 'Remove'. At that point it becomes apparent why you cannot just hit the delete key, you need to consider what happens to existing users. Do you let existing users carry on using the software, or do they have the package whipped away from under their feet?

Windows Settings Section

From the policy creator's point of view, this section is disappointing. Why so? Because almost all the security settings are configured at the domain level, not the OU. Whilst logon scripts are still useful, most of the scripts are assigned under the User Configuration, rather than the Computer Configuration.

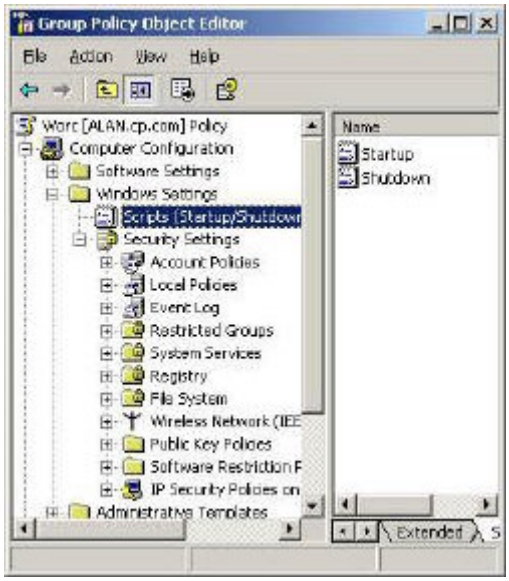
In contrast to this page, the User Configuration, Windows Settings has a much richer seam of policy folders.

Group Policy Topics

Computer Configuration

Software Installation

- Startup Scripts
- Shutdown Scripts
- Security Settings
- Event Log - Maximum size



Scripts

Whilst logon scripts have been around for ever, Startup and Shutdown scripts are new in active directory.

In truth, I am still waiting for a 'killer application' for Startup and Shutdown scripts. Most of the scripting jobs are carried out in by Logon and Logoff scripts in the User Configuration settings.

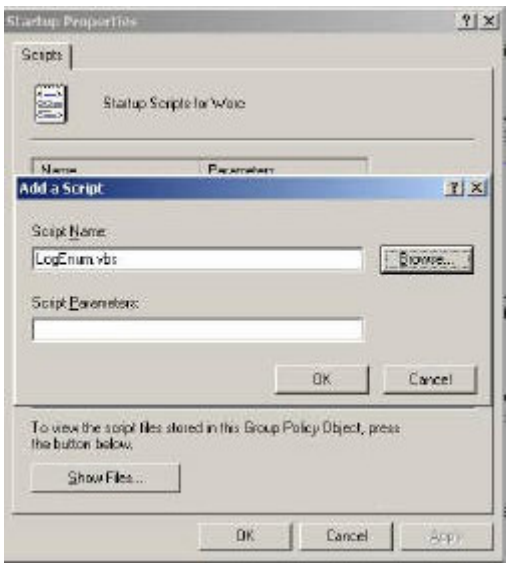
With scripts there are three distinct tasks.

Deciding what the script will do.
Writing the script using VBScript.
Assigning the Startup scripts via group policies.

Startup Scripts

Presuming that the scripts have been written, all we have to do is add the .VBS file to the policy box. I find that it is much better to copy the script into memory **before** you open the policy box, than to try and navigate once the box is open.

My point is that I would prefer to right click and paste, rather than use the Open and Browse option.



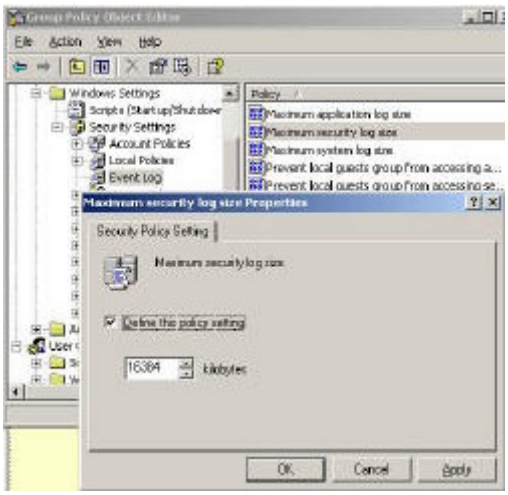
Shutdown Script

As I mentioned earlier, I am still waiting for a major use for this type of computer script.

Security Settings

Trap: Security policies for domain users must be applied at the domain level. Do not be deceived into thinking that you can have different password length and lockout policies for each OU. Wrong. I repeat you cannot use the settings in an Organizational Unit to apply security policies. In fact I was so enraged that I researched the matter, apparently these OU security policies only affect people who logon with LOCAL accounts - not domain accounts.

So, most of these settings are deceptive in that they will not 'bite' on domain users.



Event Log - Maximum size.

Perhaps the one setting that you could profitably employ would be the Event Log size.

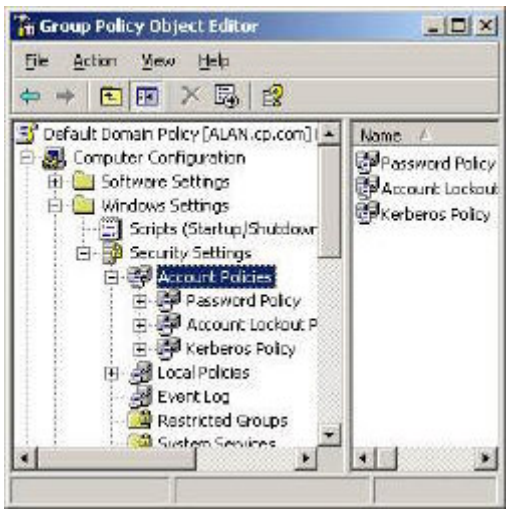
The picture shows how to increase the Security Log to 16 Mb. If you prefer bigger logs, then you could repeat this procedure for the Application Log.

Do remember the old trap; this policy only applies to computers in THIS OU and not to those in the default Computers Container. Also remember here is where are your domain controllers are stored - in the Domain Controllers folder. Unlike the Users folder, the Domain Controllers container has its own Default Group Policy.

Security Settings - Account Policies (Domain Level)

Perhaps you are familiar with setting password length and account lockout from your NT 4.0 days? This section will guide you through these and many more security policies for Active Directory Users.

Do remember that the Account Policies on this page must be configured at the Domain level. If you try to set these polices for an OU, then you will be disappointed. This is because the Security Settings at the OU level have no affect on Domain Users.



Security Settings

Account Policies

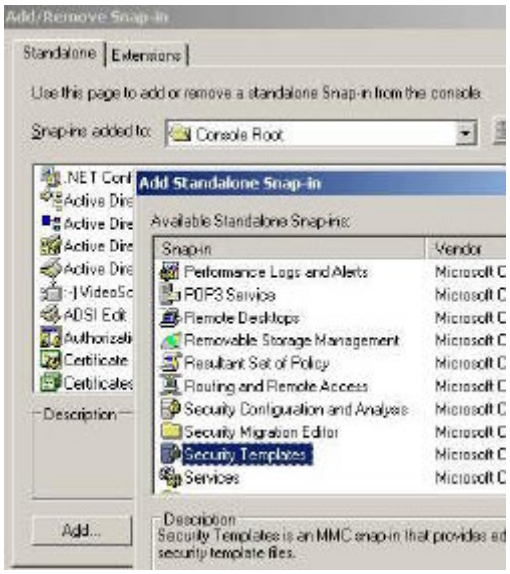
- Password Policy
- Account Lockout Policy
- Kerberos Policy

Security Settings

Before you start experimenting, I urge you to take advantage of Microsoft's built in templates. What I suggest is that you add the Security Template snap-in to your MMC.

Inside the template folder are half a dozen files with settings for each type of machine. The first task is to choose the nearest template to your situation, for example 'securedc' would be suitable for a domain controller. Once you have selected a template, then immediately right click, 'Save AS', and give it a new name, for example MyDomain. This technique will preserve the built-in settings so that you can always start again with a clean template.

Your chosen template will act as a base for creating your own Security Settings. When you are happy with your policy, load your settings with the Security Configuration and Analysis snap-in (see diagram).



Tip If you get in a pickle with Security Settings, revert to the 'DC Security' template, that's the easiest way of removing all policies. As 'DC Security' is just a blank shell, this template neatly resets your mistakes, and lets you start again.

Account Policies

* Guy's Top Three Password Policies

Minimum Password Length
Enforce Password History
Account Lockout Threshold

Password Policy

This password section really does come as a package; I will explain why you need to consider how these policies interact as we go along.

The first decision is, 'Minimum Password Length'; 8 letters is considered long enough by most security experts. To make it harder for hackers to guess passwords you can enforce - 'Passwords must meet complexity requirements'. This means that the word must contain 3 of these characteristics, UPPERCASE, lowercase, number or non-alphanumeric e.g. £ @ symbols.

At first I thought that it would be too much to expect people to remember such complex passwords, but as time went on I realized, we humans are a most adaptable animal and we do learn to cope with passwords like P@ssw0rd or better a phrase like: B££r & sk1ttl£s.

Once we set the length and complexity, the next decision is how often do users have to change their passwords? 60 days, 90 days - you decide. To prevent users just switching between two passwords, you can set * 'Enforce Password History'.

Just when you think you have the users under control, some 'clever Dick' Just when you think you have the users under control, some 'clever Dick' cycles through 24 passwords in their tea break and comes back to the original password. To stop them 'thumbing their nose' at you, fix the minimum password age at 1 day. If you set the 'Minimum Password Age' too long, then that can create new problems. Specifically, if the user forgets their old password and they are given a new password which must be changed at first logon. No can do. They would either have to wait days to logon, or else the support staff would have to remove the tick next to 'Change Password at logon'.

Account Lockout Policy

Controlling Account Lockout is a tricky and contentious area. My advice is to set the 'Account Lockout Threshold' to 7-9. Most administrators prefer a value of 3, but I would argue that 7 or more attempts will give the users more chance to remember their password without compromising security.

Enabling 'Account lockout duration', means that the account will unlock itself after the time you choose. This would save work at the help desk, but make the system less secure than if an administrator has to manually reset locked accounts.

Probably the hardest policy to explain is the 'Reset Account Lockout after'. Take the scenario where you know the lockout threshold is 3, you have got the password wrong twice, you pause to think. 'If I try again and get it wrong, my account will be locked out and I will have to ask the administrator nicely to reset my account. Or, I can wait half an hour and so have the full three chances to try my passwords again.'

Kerberos Policy

Best to leave these policies as their defaults - not configured. However, if logon is troublesome and especially if you start getting Kerberos errors in the Event Log, then you could research the Kerberos principles and make informed decisions on increasing the ticket life.

Kerberos is named after the three headed guard dog Cerberus of Greek Mythology. The idea behind Kerberos is to minimise the need for a user's password to cross the network. The concept behind the Kerberos ticket is that all their SIDs, Group SIDS and user rights, are encrypted in the ticket. So when the user needs a resource like a file in a network share, they present their tickets, not their passwords! To investigate Kerberos, install Kerbtray.

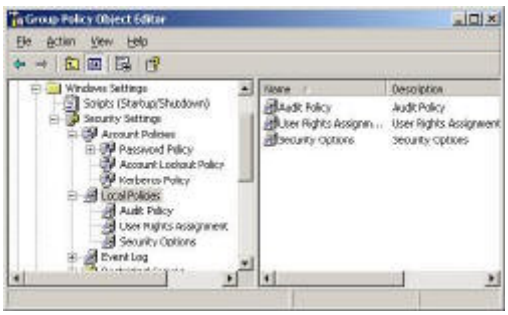
Local Polices - Audit Policy

Here is what a good audit policy will discover:

1. Who is trying to logon.
2. Which files have been deleted.
3. Who did it!

Incidentally, unlike other policy settings, these security policies do not have an 'Explain' tab, however, if you right click and select 'Help', there is a comprehensive explanation of each policy.

Trap: If you are intending to set Local Policies for your actual Domain Controller, then you should go to the All Programs, Administrative Tools, Domain CONTROLLER policy. (Audit policies for Member Servers and XP clients can be set at the Domain or OU level).



Group Policy Topics

User Configuration

Windows Settings

Account Policies

Audit Policy

- **Logon Events**
- **Object Access - Master Switch.**
- **Three administrator security settings**
- **Process tracking - a disciplinary offence?**

* Guy's Top Two Audit Policies

1. **Audit Logon events**
2. **Audit Object Access**

Logon Events

Watch out for two similar and potentially confusing policies, 'Audit Account Logon events' and 'Audit Logon events'. The difference is that Audit Logon events (the shorter one) means that you are checking who is pressing Ctrl Alt, Del at the domain controller (or desktop); whereas the Audit Account Logon events (the longer one) generates an event every time a user connects to that server across the network.

In terms of strategy, decide whether you simply want to record logon failures - possible illegal access attempts, or whether you also need to audit success.

Once you enable security policies, check the Event Viewer's Security Log (not system log) for user activity. Another tip: once you become serious about security, increase the size of the log from 512 K to at least 10 Mb.

Object Access - 'Master Switch' for file and folder auditing.

If you need to record who is accessing shares, or who is deleting files, then first you must enable, * 'Audit Object Access'. Only when you have thrown the Object Access 'master switch', can you start checking who is doing what to your folders and printers.

Three administrator security settings to consider

I have lumped together, account management, privilege use and directory service access. These are three settings that only big companies need to audit. It is all well and good recording lots of events, but ask yourself, 'Who will have the time to scour through zillions of events?' Better to record only essential settings, that way, you will easily spot security breaches.

Process tracking - A disciplinary offence?

If you enable process tracking you should get the sack! Stern words to make a serious point. My point is that Auditing eats up CPU cycles, in fact, process tracking is so intensive that your server will grind to a halt. Perhaps you can see why I would forbid process tracking. People then ask me 'Why would Microsoft include process tracking if it's so crippling?' The answer is so that developers can troubleshoot their new programs.

Local Policies - User Rights Assignments

The first thing that you notice is just how many User Rights that Windows Server 2003 provides. Consequently, there is something for every aspect of security in this folder.

A classic 'vanilla' installation of active directory will function adequately without you having to change any of these settings. The reason why you may never have to configure this section, is because many of these user rights are bestowed on people through membership of the appropriate group. For instance, place people who need to backup files in the backup operator's group. One company foolishly created a TechAdmin group and spent ages adding important rights, not realizing that there was already a built-in Administrators group which did the same job!

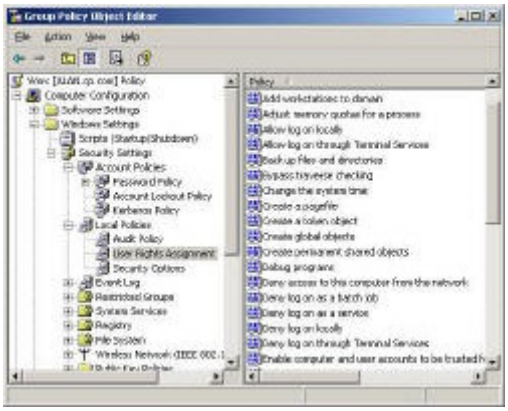
Group Policy Topics

User Configuration

Windows Settings

Local Policies

Audit Policy



What then is the benefit of these settings? I would divide User Rights into three categories:

1) Rights for special accounts, example, the SQL Agent needs to Log on as a service.

2) Prevention of users getting into mischief, for example, 'Deny shutdown system' for a Terminal Server.

3) Specialist rights for one off situations, for example, allow roll-out team Add Workstations to domain. (But not make them full administrators)

* Guy's Top Three User Rights Policies

Disable Shut Down System - Terminal Server
Disable Restore Files and Folders - Stop Backup operators sneakily restoring
Logon Locally - Testing accounts on a Domain Controller

Rights for special accounts

When you create service accounts you may wish to fine tune their capabilities. Such accounts are used by SQL and older versions of Exchange. The danger is that because service accounts are not allowed to change their password, they are a magnet for hackers to attack. More often than not, these service accounts have traditional names like SQLAdmin, so hackers guess their names, crack their password and breach the system. Your last line of defence is to give these accounts only specific rights, not full administrative control.

Rights that fall into this special category are: Logon as a batch job, Logon as a service, Enable Computer Accounts to be trusted, Increase Scheduling Priority and possibly, Lock pages in memory.

Prevent users getting into mischief

1. Deny logon through terminal services.
2. Disable, Shut Down System, so that ordinary users cannot power off the very Terminal Server that provides desktops for them and their colleagues.
3. Disable Restore Files and Folders, so backup operators cannot sneakily restore the HR database. My point is that if you had to restore files, most likely you would call upon a top administrator, not a humble backup operator.

Specialist Rights for one off situations.

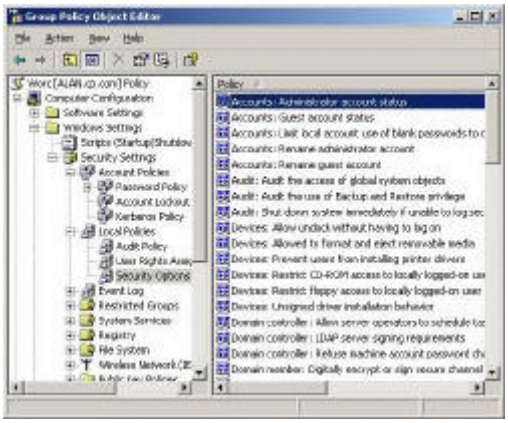
1. Add Workstations to the Domain. Better to give the roll-out engineers limited rights rather than making them full administrators. By default users have the right to add 10 workstations to the domain without any extra rights.
2. Allow right to logon locally. When you only have a DC available to try out newly created user, you need to give those accounts this right. However you could make the test accounts backup operators who do have the right to logon locally.
3. Modify firmware. Possible scenario, you have an outsource team who need to upgrade the hardware.

Local Polices - Security Options

Security Options is an apt heading. Lots of protection and certainly zillions of choices. Working your way through these policies will help to clarify what level of security you need, low, medium or high.

Remember that the more security that you implement, the more work there will be for the administrator. Therefore, I would resist high security settings unless your directors demand the highest protection.

Local Policies



Audit Policy
User Rights

Security Options.

1. **Administrators account**
2. **Devices**
3. **Interactive Logon**
4. **Network**

* Guy's Top Three Security Options

1. **Accounts: Rename Administrator account.**
2. **Do not display last user name**
3. **Require Smart Card Logon**

Administrator's Account

Probably the most important security question is: 'What are you going to about the Administrator account?' The problem is that this built-in account is a liability because hackers know that: If it's a Windows operating system, then there will always be an Administrator account to hack. The answer is to * 'Rename Administrator Account', and possibly to disable the 'Administrator Account Status'. Naturally, create a new administrator, but choose a name that blends in with the other user accounts.

Tip (Double) check that double negatives do not obscure your objective for the administrator's account.

Other Security Options are neatly categorised thus:

Devices

You really should come to a decision about unsigned device drivers, my guess is that as time goes on, it will be more important to allow only signed, approved, certified drivers.

Domain Controller

Trust me, there is nothing for ordinary mortals here. Specialist policies only.

Interactive (Keyboard) Logon

The policy * 'Do not display last user name', causes emotions to run high. The two sides of the argument are:

1) That on communal machines one user can inadvertently lockout another user's account. What they do is keep their head down and not see that someone else's name is in the logon box, as a result they accidentally type in their password for the other person's account. The result is a colleague's account is unfairly locked out. So enabling 'Do not display last user name', will prevent that particular user error.

2) On the other hand, enabling 'Do not display last user name' for machines where the same user always logs on, only causes frustration and resentment. This is because it's really unnecessary for anyone to type in their username at every logon if no-one else ever sits at that computer.

A prediction, one day we will all use smart card logons, the only debate is what form they will take, finger print, credit type cards or retina scan (yuk). So, my advice is to put Require Smart Card Logon on your 'To Do' list.

Microsoft Network

By now you will have come to a decision on whether you are a high, medium or low security company. Only high security organizations will need these specialist settings for certificates.

Network Access for client and server

Useful settings here, policies which will assist you in keeping out the bad guys without affecting the good guys. For example, if you disable remote registry editing who will that affect? Only the bad guys.

Recovery Console

Just two settings. Control the Shut Down without logon button, and decide on clearing pagefile on shutdown. The later will mean it takes slightly longer to reboot, but the system will be more secure.

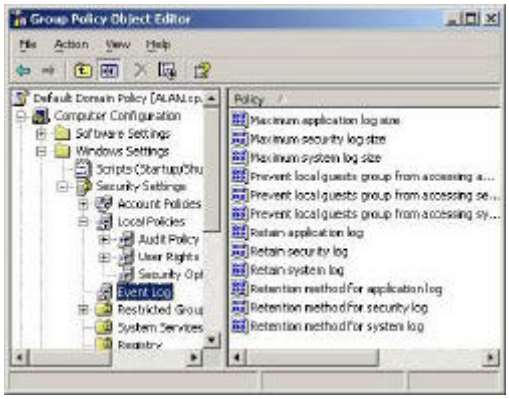
System

Frankly, another specialist section which you would only need to visit rarely. Make that extremely rarely!

Security Settings - Event Log

A set of uncontroversial, yet helpful policies which shape your three main event logs.

Security Settings



Event Log

1. Log Size
2. Retention Method
3. Retain Period
4. Prevent
5. local guest groups from accessing logs

* Guy's Top Two Event Log settings

1. Log Size
2. Overwrite events as needed

Log Size

Since NT 3.51 days the default log size has remained at a mere 512k. (kilo, not megabytes). Why not create a policy which increases all logs to at least 4,000k = 4 Mb? Small logs size risks later events overwriting early ones and so you miss valuable troubleshooting clues. What have you got to lose? Surely you can afford a relatively tiny amount of disk space. These days more and more programs write events to the application log, so do not just increase the system log, but also remember the application and security logs.

Retention Method

Choose 'Overwrite events as needed', rather than overwrite every 7 days. By selecting this policy, coupled with increasing the log size, you will minimise missing events in the logs.

Only high security organizations need, 'Do not Overwrite, clear logs manually'. The idea is that being very security conscious, you do not allow any event to go unrecorded. However, if you select this option, then when the logs fill up, the system grinds to a halt until an administrator clears the logs. Here is another case of the more security you have the more work for you.

Retain Period

If you take my advice and use the 'Overwrite events as needed', then you do not need these settings. Their purpose is to fine tune those who like to overwrite the logs after x days. Here is where set that value for x.

Prevent local guest groups from accessing logs

Here is an example of what I mean by a gentle and uncontroversial policy. What you can do is hide the logs from Guests who log on to the machine. My thinking is not many guests are likely to logon, even if they do they are not going to see the company secrets by viewing the system log. Only administrators can see your security logs, so even without this policy guests could not snoop there.

Security Settings - Restricted groups

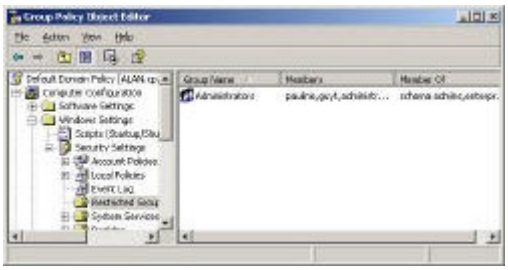
From a technical point of view this is a curious policy. To start with there is no policy - you have to create one. Fortunately, creating a Restricted Group policy is easy. However configuring can be confusing as there are two similar properties, Members and Member Of.

The plain 'Members' list defines who belongs to the restricted group. Whilst the 'Member Of' list, specifies which other groups the restricted group itself, belongs to.

When you enforce a Restricted Groups policy, any current member that is not on the Members list is removed. Equally, any user on the Members list who is not currently a member of the restricted group is added to that group.

The 'Reverse membership' configuration ensures that each Restricted Group is a member of only those groups that are specified in the Member Of column.

Implementing Restricted group policy.



As ever, when you are not sure what to do, right click on a folder. So, from the Restricted Group folder, right click, Properties, Add Group. Next make your selection for the Members and Members Of boxes.

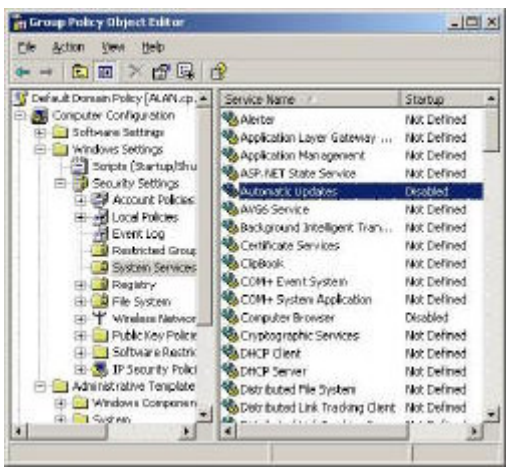
Now that you understand how restricted groups work, you come to the strategic decision about how to implement them. The philosophy here is that you do not want anyone to sneak in extra members of key groups such as administrators. You can extend the principle to politically sensitive groups that you created, for example Mangers, Bosses, or Downsizing Committee.

Who needs this policy? Companies that are so big that you have lots of administrators and you want to control membership of key groups.

Security Settings - System Services

Something different. Policies that affect the operating system rather than the users. If you are familiar with the Services snap-in, then you may already have ideas about which services should be disabled, for instance Telnet, and FTP.

Security is our watchword in this section, so let us disable services that will never be needed, especially if they could be used by hackers.



* Guy's candidates for services to disable

FTP
Trivial FTP
Telnet
Computer Browser
WWW Publishing

Services where you need to decide

Error Reporting Service
Automatic Updates
Remote (Various)

Configuration

Take the time to go through the list and decide which services to disable with a policy. Once the machine starts, you can over-ride the policy, simply go to the Services, double click the particular services and select one of these start-up options:

Automatic
Manual
Disabled.

A final thought, rather than being negative all the time, why not seek out services that you positively wish to set to Automatic Startup? 'Special Administration Console Helper' springs to mind.

Group Policy - Software Installation

With software installation policies you get the best of both worlds; the ability to roll-out programs like Word, Access and Excel to local machines, while retaining central control of all such desktop applications. For example you could assign a program to a group of secretaries, but when they get a promotion, you could assign them additional accountancy software. This avoids running programs across the network and saves you running around to each machine in the building every time a setting needs changing.

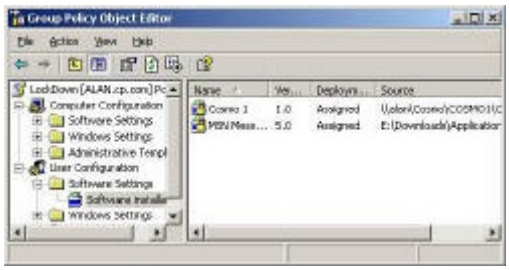
While it is possible to assign software to computers, I prefer to assign packages here in the User Configuration section of the GPO (Group Policy Object).

Group Policy Topics

Getting Started - Assign your package

As a pre-requisite you must obtain the programme in .MSI format. Then you share out the folder containing that .MSI package.

To create the policy, right click 'Software Installation', choose, New, Package, and simply browse for the UNC name of the server \\ alan\Cosmo.



Trap 1: Instead of choosing a UNC path (correct), you use a local path. In the picture, compare Cosmo (correct - UNC) with MSN Messenger (wrong - e:\download)

When you configure your package there are two possibilities, Assign (best) or Publish. With Assign, an icon appears on the Start Menu and when the user clicks, the program is installed. Contrast that with Publish, where the user would have to go to the Control Panel, Add or Remove Programs before they could install the program. Now, you can see that 'Assign' is easy for the users, whereas 'Publish' has many more steps. Also 'Assign' is able to take advantage of elevated rights, so that ordinary users in effect can install the programs that you assign to them.

Product life-cycle

With a Software Installation Policy, the real savings come when you analyse the full life cycle of a software package. When you first install a new program you cannot believe that one day it will be out of date, you also put to the back of your mind that it may need a service pack. Providing you assign software through group policies, upgrade and removal are just a matter of a few clicks. You certainly do not have to visit every desktop. Unfortunately, you cannot remove or upgrade software that was installed manually, out side the scope of the group policy. So the message is, plan for the software life-cycle and use this smart software installation technology.

Upgrading

If you need to update your software package, right click, properties and you will see the selection of tabs opposite.

Trap 2: Be careful when you right click and select properties. The blue and white box called 'Software Installation' has its own properties; these are in addition to each . MSI package which has its own properties. My message, be careful where you right click.

When the time comes to upgrade, go back to the server and add the . MSI to the network share and select 'Assign', just as you did with the first package. Now comes the crucial step, select the Upgrades tab and add the name of the second program. Make sure that you get the logic right, you do not want to replace the new program with the old one!

Deployment

There are options for fine-tuning your deployment strategy. I particularly like the ability to remove the application when the user move out of scope, for instance, if they move to a new OU.

Categories

These are only used if you are publishing. Guy says avoid publishing!

Group Policy - Windows Settings Section

This Windows Settings section probably has the widest range of Group Policies, including one or two surprises.

Group Policy Topics

User Configuration

Windows Settings

- Remote Installation Services
- Scripts (Logon / Logoff)
- Security Settings (Set elsewhere)
- Folder Redirection
- Internet Explorer
- Maintenance

* Guy's Top three Policies for Windows Settings

1. * Logon Scripts
2. * Folder Redirection
3. * Internet Explorer Maintenance - Proxy server setting

Remote Installation Services (RIS)

Sadly, for most people, RIS will be a matter of saying, 'Yes I understand what the settings are for, but actually, I do not need them'. Sad, because RIS is one of THE great services, however since Ghost is so well established administrators are unwilling to believe there is a better solution.

If you are using RIS, then I would recommend enabling 'Automatic Restart', it's helpful if the service fails for RIS to try again. The only other setting I would change is disabling the 'Custom Setup', you do not want users fiddling with your installation.

* Scripts Logoff has its own section

Security Settings

This icon is not what it seems. The main security settings are not configured here but from the **Computer** Configuration. Moreover, settings such as password length are set at the **Domain** level, not at the OUs.

The security settings here are merely a shell for consistency, there is little if anything to be gained by setting policies here. If you need account policies settings such as passwords, then go to the Default Domain policy, Computer Configuration. That means navigating away from the test OU.

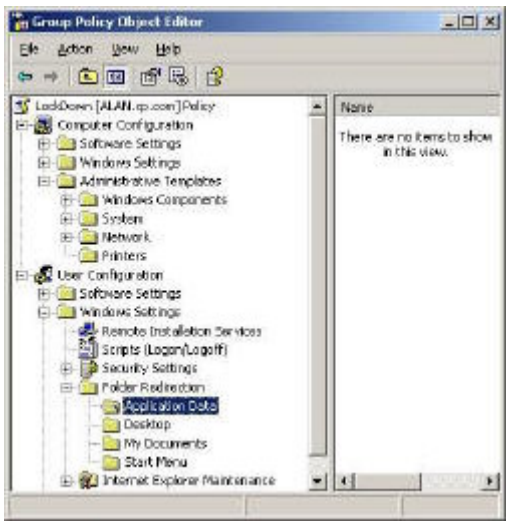
When I research these seemingly useless settings, I discovered they are used in one specialist scenario, when users authenticate locally in the SAM database, rather than logging on to the domain. In other words, if users select the machine name rather than the domain name in the logon box, then these settings bite. One possible use for these settings is SQL Member servers.

Folder Redirection has its own page

Internet Explorer Maintenance has its own page

Group Policy - Folder Redirection

Folder Redirection is one of the undiscovered gems amongst the myriad of group policies. When you configure the file locations of saved files, mastering folder redirection will enable you to take shortcuts. Let us remind ourselves of where Office programs save their files; by default, all files are directed to the My Documents folder. What do people do? Redirect the file save location to the home directory. To complete the circle the administrator must now map a drive to the user's home directory. Perhaps now you can see what I mean by taking a shortcut? In one fell swoop, you can redirect the My Documents to the server and forget about mapping network drives for home directories?



Group Policy Topics

User Configuration

Windows Settings

Folder Redirection

[Application Data](#)
[Desktop](#)
[My Documents](#)
[Start Menu](#)

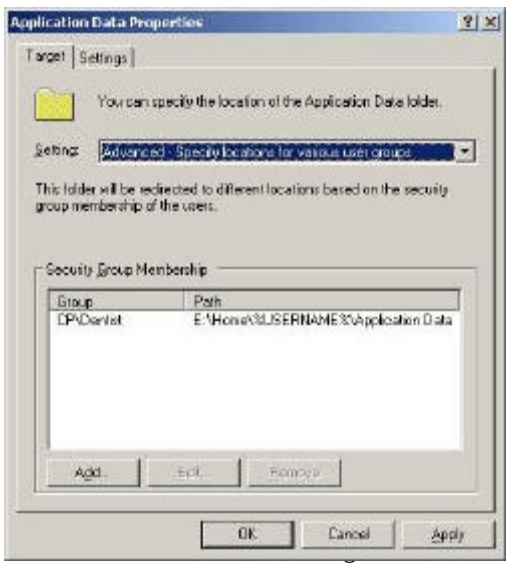
Application Data

What we are configuring here is client side caching. My view is that normally, clients can adequately cache their own programs locally. This Application Data setting is different from the Folder Redirection for the 'My Documents'.

Desktop

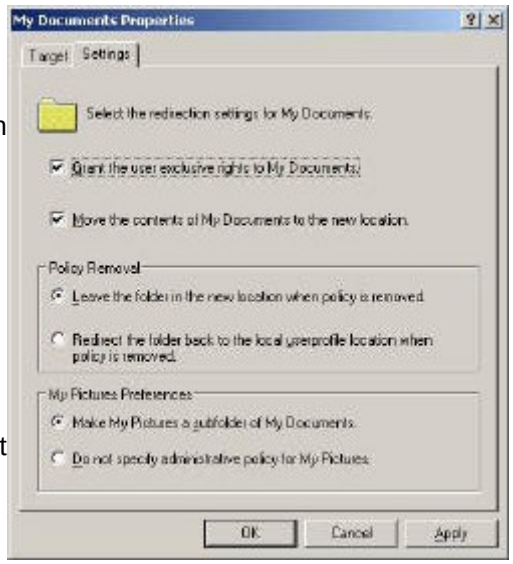
There is a knack to configuring all these 4 redirection settings. At first, it seems as though there are no policies in the container. However, if you right click one of the yellow folders and select Properties, then a rich selection of settings comes into view.

From the first menu, select Target, now drop down the Settings box and choose: 'Advanced - Specify Location for various user groups'. Choose this setting where you would not normally want all users to share the same folder.



If you are organized, then you would have shared out the redirect folder on the server. However even if you haven't, you can still choose the group you intend to redirect. As you share out the folder on the server, so the path changes to the famous %UserName%. Permissions permitting, the subfolders are created automatically thanks to %UserName%.

My Documents



Whilst the My Documents are probably the most import redirection setting, the principles are much the same as the previous folders. What I would like to concentrate on here is the Settings Tab.

Once again, Microsoft have thought of everything. What I particularly like is the control you have over moving the files, and there are even options for what do to if the policy is removed.

Finally, at the bottom you have decisions on what do about the My Pictures sub folder.

Start Menu

The start menu uses the same technology as the other folders. The one change that I suggest here is to point everyone in the group to the SAME folder. The strategy is then to fill this folder with Start Menu icons. There is no need for the %UserName% variable, instead why not give all the users in the group the same Start Menu experience.

Where you have subfolders off the Start Menu, no worries, like good children, they follow their parent folders automatically!

Group Policy - Internet Explorer Maintenance

This section is fore administrators who want advice on how to control Internet Explorer settings with a group policy. There are about a dozen main IE settings, if you would like advice on which are with bothering with, check Guy's advice at the end of each component.

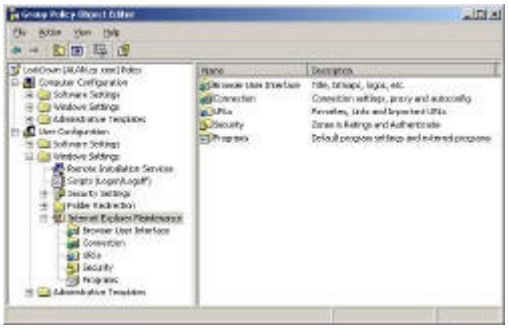
Group Policy Topics

User Configuration

Windows Settings

Internet Explorer Maintenance

Browser User Interface
Connection
URL
Security
Programs



There are three places where you can configure Internet Explorer policies. Some say that there are over 700 policies in Server 2003, it feels like there are 200 just for Internet Explorer. Here are the three sections which specialize in IE, they are listed in my order of importance.

1. User Configuration, Windows Settings, Internet Explorer Maintenance (Best)
2. User Configuration, Administrative Templates, Windows Components, Internet Explorer
3. Computer Configuration, Administrative Templates, Windows Components, Internet Explorer

1.User, Windows Settings, Internet Explorer Maintenance (Best)

The internet explorer is ripe for group policies. This section has a good mixture of policies which lock down the user, coupled with policies to spoon feed them with sensible defaults. For example, controlling the proxy server and setting the home page.

* Guy's Top Three IE Maintenance Group Policies

1. Connections - Proxy Settings
2. URL - Important URLs
3. Security Zone - Content Rating

Browser User Interface

This section is just cosmetic. Perhaps it's worth the effort configuring if you are a large company or wish to impress your users or customers. Guy's advice - ignore.

Connection

*** Proxy Settings**

Most intranets will benefit from controlling the proxy server IP and ports. Use a group policy to centralize these TCP/IP numbers. Guy's advice - must configure this setting.

Automatic Browser Configuration

Useful for checking for updates. Tricky setting - worth a look, especially when a new version of IE is released.

Connection Settings

You do not want users fiddling with modem settings, so manage any connections through a group policy. Watch out for a check box which allows you to delete old modem settings. Guy's advice - useful for users with dial-up connections.

User Agent String

Used for tracking statistics. Guy's advice - specialist use only.

URL

*** Important URLs**

Here is where you can set the Internet Explorer's 'Home Page'. Setting the Search Engine and online support will also benefit users. Guy's advice - always set these policies.

Favorite and Links

You may consider configuring these links centrally for all users. Keep the most important sites near the top of the users search path.

Security

*** Security Zones and Content Rating**

Today, all companies have views on what is appropriate surfing, here is where you control which sites are allowed. Guy's advice - must check.

Authenticode Settings

Not sure that you need these. Specialist application.

Programs

The programs folder has mundane policies, nothing earth shattering here. Worth checking that Outlook Express is the Newsgroup editor otherwise the defaults will be O. K. Guy's advice - harmless setting, but you may as well take control and set.

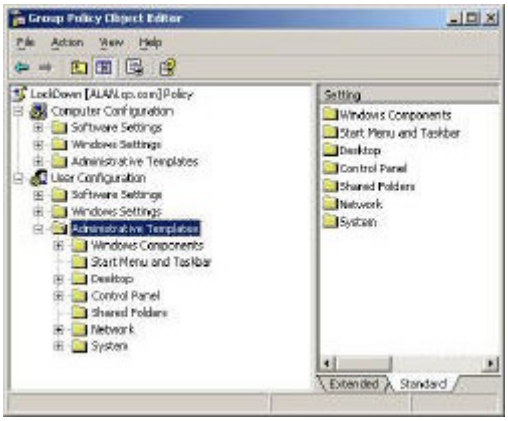
Group Policy - Administrative Templates

This section deals with the classic group policies. If you are new to group policies, this is the best place to start. Cut your teeth on policies which are easy to understand, and fun to implement, for example, 'Disable the Run Command' or 'Hide all icons on the desktop'.

While many administrators get fixated on policies which remove tabs, I find it satisfying to discover settings which improve users' productivity, for example 'Run Programs at Logon'. As I look through the hundreds of policies I became aware that most of them would only be useful in specialist situations. What I have done is to highlight those policies that are worth considering on a medium secure network.

Note: There are two sets of Administrative Templates, one for Users (this page) and one for Computers. The User Configuration folder has the richer set of policies.

Group Policy Topics



Administrative Templates

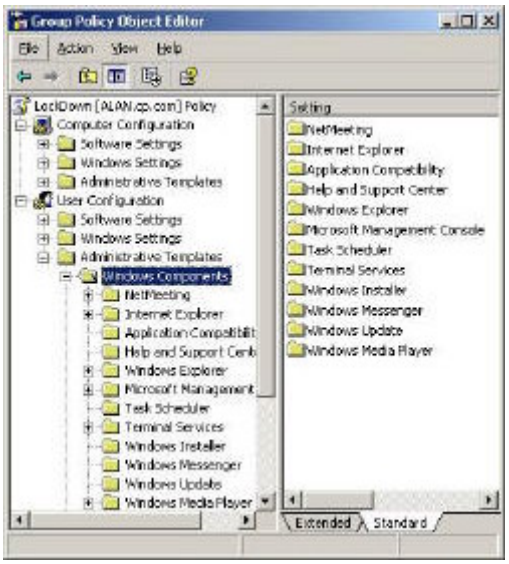
Windows Components
Start Menu and Taskbar
Desktop
Control Panel
Shared Folders (nothing of interest)
Network
System
Windows Components

Pre-requisites before creating your User Group Polices:

1. Access to a Windows Server 2003 domain controller. (Windows 2000 has different menus with fewer settings.)
2. Install Group Policy Management Console (GPMC).
3. Dedicate a test OU for your experimental policies. (Not essential, but safer than using the default domain policy)
4. Create a Group Policy (GPO).Right click your policy, then edit.
5. Navigate to the User Configuration (not Computer). Next expand the Administrative Templates.

Group Policy - Windows Components

Each Windows Component folder has specific policies for that application, for example, timeouts for Terminal Services. Whilst there are numerous settings here, I anticipate that you will only need a handful of these policies, the trouble is that each system requires different applications and so there is no one size
fits all.



Group Policy Topics

Administrative Templates
Windows Components

- Netmeeting
- Internet Explorer (Own Section)
- Application Compatibility
- Help and Support Center
- Windows Explorer
- Microsoft Management Console
- Task Scheduler
- Terminal Services
- Windows Installer
- Windows Messenger
- Windows Update
- Windows Media Player

* Guy's Top Five Group Policies for Windows Components

1. Do not allow the 'Did You Know' content to appear
2. Remove "Map Network Drive"
3. Start a Program on Connection
4. Always install with elevated privileges
5. Windows Media Player

Netmeeting

To date, I have found that the only way to start NetMeeting is: Start, Run, Conf. When I see NetMeeting, I think of training sessions, however I am sure that there are business functions for this program.

Meanwhile back at Group Policies, we find the usual array of 'Disable' settings so that users cannot fiddle with the buttons when they should be watching the conference. If your Network only makes casual use of this conferencing program, then I would not bother configuring these policies.

Internet Explorer

There are so many important settings for Internet Explorer, that it has its own IE pages

Application Compatibility

Just one setting here - Disable 16-bit applications. Why would you need this? One answer would be to prevent old programs destabilizing the operating system. Other than the observation - 'Why would you need a 16-bit program in 2004? ' -I would ignore this folder.

Help and Support Center

Again, only one setting - * 'Do not allow the 'Did You Know' content to appear'. This section of the Help Center is only available if you have internet connection. So, if your users cannot connect to the internet, then changing this setting will speed up 'Help and Support'. Beware of double negatives, you really must test that your logic matches the policy's logic.

Windows Explorer (Not to be confused with Internet Explorer)

More than 30 settings, including the classic - * 'Remove "Map Network Drive". 'Lots of other restrictive policies, consider removing tabs such as DFS, Security and Hardware from the explorer.

The key is to balance users' ability to browse for vital resources, while preventing them from getting into mischief. Make decisions here based on your overall philosophy of the desktop, rather than in isolation. By that I mean, if you restrict browsing the network, then compensate by providing mapped network drives.

Microsoft Management Console

This is about restricting which Snap-ins are available to the MMC. Keep in mind that many of the Snap-ins will not function in the hands of non-administrators, so what you are doing here is tightening up the selection of what administrators will see if they try and create an MMC. Guy's advice, ignore this section.

Task Scheduler

The settings here are virtually identical to the Computer Configuration. However the question remains, do you give users the responsibility of scheduling maintenance programs like backup? Probably not.

Terminal Services

It has to be a good idea to set idle time-outs. In fact, this whole Terminal Services section is a chance to be positive and improve the user's experience. For example, * 'Start a program on connection'. Note there is a much bigger collection of **Terminal Services policies** under Computer Configuration.

Windows Installer

* 'Always install with elevated privileges' will ensure that programs will install properly without you having to logon as administrator. I have seen administrators placing users in powerful administrative groups, just because they did not know about this elevated privilege setting.

Trap: 'Elevated privileges' must also be enabled in the Computer Configuration for it to be effective.

*Windows Messenger

Here are two useful settings to control how Windows Messenger behaves. Firstly, are you going to allow Messenger to run - at all? If you do permit the Messenger to operate, would you wish it to start automatically?

Windows Update

Do you like Windows Update? No? Well if you hate it here is your chance to disable the Update service and so prevent it hunting for new patches.

Window Media Player

This section provides all the Group Policies necessary to create the optimum Media Player environment. Helpful features include specifying proxy settings, coupled with restrictions to hide unnecessary tabs. Incidentally, these policies in this folder are controlled by its own . adm template called WMPlayer. adm.

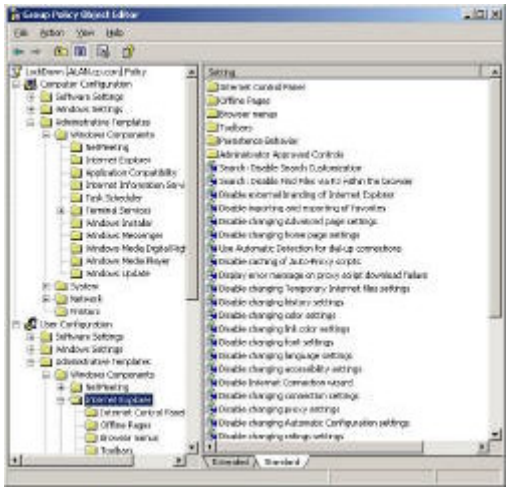
Group Policy - Internet Explorer for Users (2)

This section is mainly about tying down the user rather than being 'Mr Nice'. If you like wearing the 'Mr Nasty' hat, then there are lots of group policies for you to screw down the users.

There are three places where you can configure Internet Explorer policies.

1. **User Configuration, Windows Settings, Internet Explorer Maintenance (Best)**
2. **User Configuration, Administrative Templates, Windows Components, Internet Explorer (Here)**
3. **Computer Configuration, Administrative Templates, Windows Components, Internet Explorer**

Group Policy Topics



Administrative Templates
Windows Components
Internet Explorer Root

Internet
Control Panel
Offline Pages
Browser menus
Toolbars
Persistent behaviour
Administrator Approved Controls

3.Computer Configuration for IE

* Guy's Top Three IE Group Policies

1. Disable Attachment Download from Outlook Express
2. Disable Save Program To Disk
3. Administrator Approved Controls

Root

Put blinkers on the users, is the theme of this section. For example, force users to concentrate on their jobs by stopping them from changing the Proxy addresses, Ratings, Connections and many similar areas.

Companies with Internet Browsing policies will love this section. Alternatively, you could turn the situation on its head and design your office paper based policy using ideas copied from these Group Policy settings.

* Disable Attachment Download from Outlook Express could be worth considering.

Be careful with 'Disable AutoComplete forms', I think it mean to stop forms saving passwords and usernames that people use regularly. I say be careful, because I really like being able to save my username and password, that way, I do not having to keep typing it in every time I visit a site.

Internet Control Panel

Once again 'Disable' is the theme. You can prevent the users from even seeing tabs like security and content in Internet Explorer. In addition, you can even control what the users can do thought the Computer Configuration settings.

Offline Pages

Do you really want to disable users from saving pages? Probably, if the machine is a kiosk or in a public area.

Browser Menus

If you are serious about security, then you will need to disable the ability to *Save Program To Disk. As for the rest of the group policies, they seem pretty harmless to me and, I cannot make a good case for disabling many of these settings.

Toolbars

I like the Alexa and Google toolbars so I would be dismayed if a policy denied me these useful aids.

Persistent behaviour

Here is where you can set limits on files saved from various zones. Useful when short of disk space. Worth setting if you are going to restrict the internet temporary files in general.

* Administrator Approved Controls

Here we are talking ActiveX. The danger is that rogue ActiveX code could cripple a machine. What these policies will do is help you Approve Zones where users can run Chat, Shockwave, Media Player and similar 'Real Time' programs.

3.Computer Configuration, Administrative Templates, Windows Components, Internet Explorer

Only use these settings if you wish to 'fine tune' the Internet Control Panel in the above User Configuration, Administrative Templates. 90% of the IE policies are taken care of in the User Settings.

'Make Proxy Server per machine' - may be worth considering.

Group Policy - Start Menu and Taskbar

Here is a classic selection of policies to shape the users experience of Windows XP or 2000 Professional. Combine the science of securing the desktop, with the joy of mastering group policy settings.

Group Policy Topics

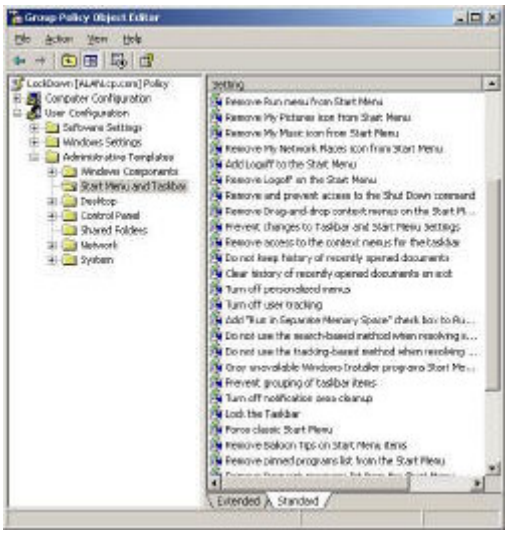
Administrative Templates
Windows Components
Start Menu and Taskbar (Note Taskbar not Task Manager)

* Guy's Top Three Group Policies

1. **Remove the Run Command**
2. **Add Logoff to the Start Menu**
3. **Remove my Network Places**

Start Menu and Taskbar (Note Taskbar not Task Manager)

These Start Menu settings remind me of where policies started - with Poledit and NT 4. 0. In this section, there are over twenty policies which just remove programs or folders from the Start Menu. Take as an example, * 'Remove Run menu from Start Menu'. Ask yourself, 'Do my users need this capability? 'If you answer in the negative, then they have no business purpose for the Run Box'. However, if you remove this feature, then be sure to make all their programs available from the Start Menu.



Rather like putting blinkers on horses, restricting places such as: * My Network Places, My Music, Search and All Programs List, may make your users run faster! If you warm to this 'Mr Nasty' theme, then you could remove the clock and even hide the notification area.

In amongst all the restrictive settings is one positive item that I thoroughly recommend: * 'Add Logoff to the start menu'.

I have to say there are some 'Luddite' settings that I would not want on my network, like 'Force classic Start Menu', or 'Prevent Grouping of Taskbar items'.

'Remove Logoff from the Start Menu', is an example of specialist group policy for particular circumstance. For example, you have a Kiosk or public area machine and you want only a special user to be logged on. (One who is heavily restricted!)

Group Policy - Desktop

This section typifies the restrictive side of group policy. Take advantage of a wonderful opportunity to create a plain desktop with no distractions for the users.

Administrative Templates

Windows Components

Desktop

* Guy's Top Three Group Policies

1. **Hide Internet Explorer on the Desktop**
2. **Prohibit users from changing My Documents path**
3. **Do not add shares of recently opened documents to My Network Places**

Desktop Policies

My advice is to dovetail these desktop policies with your broader company policies. For instance, if you have a company directive that everyone should clear their desk every night, then group policies such as 'Hide All Items on the Desktop' will reinforce the corporate message.

As with the Start Menu policies, there are half a dozen objects where you can 'Remove' icons from the user's vision. For Example, remove the My Computer, My Documents and the Recycle Bin. When you have finished Removing, you can start on Hiding. For Example * 'Hide Internet Explorer on the Desktop' (If you enable this setting, then I would keep the Internet Explorer icon on the Taskbar)

One setting that I can recommend is * 'Prohibit users from changing My Documents path'. This would compliment the policy which redirects the My Documents to a network share. Another policy that is worth a look is: - * 'Do not add shares of recently opened documents to My Network Places'.

If the machine is that famous communal Kiosk, then the setting: 'Do not save setting on exit', makes sense. For all other machines, this setting will only infuriate users - so I would avoid it!

Group Policy - Control Panel

Unlike the Start Menu and the Desktop, where restrictions are optional, I would urge even the nicest of administrators to evaluate these Control Panel Policies. Remember that old saying that, 'Prevention is better than cure'? Well, never was prevent more appropriate than configuring polices to stop users destroying their monitors.

Administrative Templates

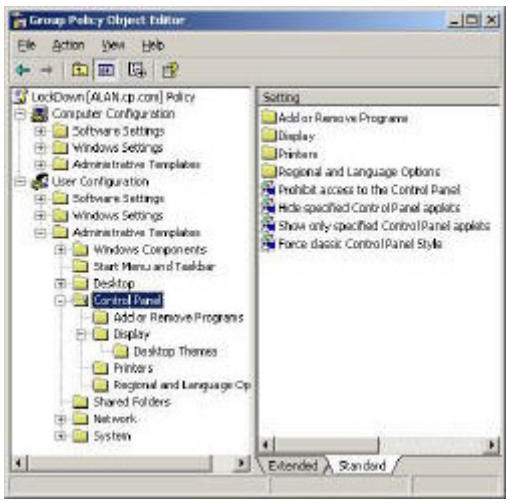
Windows Components

Control Panel

- **Add or Remove Programs (Desktop Themes)**
- **Display**
- **Printers**
- **Regional Settings**

*Guy's Top Four Group Policies

1. **Prohibit Access to Control Panel**
2. **Hide Settings Tab**
3. **Add or Remove Programs**
4. **Default Active Directory Path when searching for printers**



Control Panel (Root)

Seriously consider a group policy which will restricting users with: * 'Prohibit Access to Control Panel'.

If you wish to take a less extreme view then you have two strategies; either disable all icons, and make exceptions; or take the reverse view, enable all icons with just a few named exceptions.

Display

The most expensive hardware error that I have ever seen, is where a 'Psycho' user destroyed his monitor by fiddling with the settings. With older monitors, it is possible to set the refresh rate faster than the motor can cope with, the result is that the VDU motor burns out. I have also had reports of users setting their screen resolution to extremely high values, which caused the machine to keep crashing.

The answer to the above problem is a policy which * 'Hides the Settings tab' of the Display Icon. If you put on your 'Mr Nasty' hat, then you can 'Remove the Display Icon', or go the whole hog and disable the entire Control Panel.

On the positive side, you can make the screen saver more effective by setting, 'Password Protect the Screen Saver' and then entering a suitable timeout value.

Your company culture will determine how you regard policies in the Desktop Themes sub folder. My view is that you must balance giving users a comfortable screen, with the

potential for time wasting by constantly adjusting the settings. My choice would be to leave the Desktop Themes policies as 'Not Configured'.

* Add or Remove Programs

This is an ideal area to prevent users from adding rogue programs to their machines. Apart from wasting time, such programs always increase your support costs. If there is a good business case, then you could possibly logon as administrator and install the software. Much better would be to use a group policy to assign software using elevated rights.

Your strategy here is either to take the ruthless view and 'Remove add or remove programs', or else to fine tune which tabs are available.

Printers

Here we have examples of the opposing philosophies behind group policies. For those who like the 'Mr Nasty' role, you can stop users adding printers. However, this setting is not all it seems, for instance, it does not stop users adding printers by the back door and neither does it disable Add Remove Local printers. Would a better method be to use permissions to control network printer usage?

For those who prefer the 'Mr Helpful' role, you can set * 'Default Active Directory Path when searching for printers'. If you like these policies which customize the operating system to your network, then check the 'Browse' settings.

Regional and Language

There is only one setting here, what it does is specifically stop users selecting or changing the language settings. I can only think that you would need to bother in a very specialist scenario!

Group Policy - Network Connections

This section gives you an opportunity to befriend laptop users and help them with their offline folders. Otherwise this folder only has specialist legacy policies to control administrator's rights.

Administrative Templates

Windows Components

Network Connections

Offline Connection

Network Connections

* Guy's Top Three Network Connection Group Policies

1. **Action on Server Disconnect**
2. **Synchronise all files before logging off'**
3. **Enable Windows 2000 Network Connection Settings for Administrators**

Network Connections

Here is a section neatly divided into two parts, Offline Folders and Network Connections.

Offline Folders

Offline folders enable laptop users to synchronise local files with copies stored on the server. So, when they disconnect from the LAN, their laptop contains documents which would normally be stored on the server.

However, offline folders are a liability where everyone is permanently connected to a fast network. From a broader perspective, this maybe a reason for putting remote users in their own OU, then you could create a special offline policy for dial-in users. My assumption is that you have remote users, otherwise, ignore these policies.

* 'Action on Server Disconnect' take the trouble to anticipate what might happen if the laptop user unexpectedly loses contact with the server. Then help them by specifying what the server should do if their laptop is suddenly disconnect from the network.

* 'Synchronise all files before logging off', a useful policy which holds the users hands and prevents data loss. 'Prohibit make available offline', would be useful for folders that users should only access when at work.

Network Connection

There is a crucial 'Master Switch' here. For many of the other settings to be effective, you must first enable, the * 'Enable Windows 2000 Network Connection Settings for Administrators'. Bizarrely, this setting is at the bottom of the list, when it would be better at the top.

Taking a step backwards, in Windows 2000 you could disable network settings for administrators. Presumably this setting is for companies that are so big that you had various grades of administrator. Alternatively the company was so small that you made everyone and administrator, then you sneakily began to take away their rights.

My advice is to ignore the settings here. However if you are thinking of applying them, then be sure that you understand the logic. Another clue to avoid this section is that firstly, these are legacy settings, and secondly you would be curtailing the power of administrators!

Group Policy - System

Here is another section where every administrator will benefit from restricting the users, if only by stopping them hacking the registry. Before you start, compare and contrast the settings here with those in the Computer Configuration \ Administrative Templates \ Windows Components \ System folder.

Administrative Templates

Windows Components

System

- **User Profiles**
- **Scripts**
- **Ctrl Alt Del Options**
- **Logon**
- **Group Policy**
- **Power Management**

* Guy's Top Five System Group Policies

1. **Prevent Access to Registry editing tools**
2. **Restrict these Programs from being run from help**
3. **Code signing for drivers**
4. **Logon**
5. **Group Policy Slow Link Detection**

System (Root)

These are settings that 'Mr Nasty' will love. 'Prevent Access to the Command Prompt'. Perhaps you have already removed the run command, now you want to bolt the back door to the 'Dos Box'.

I cannot think of a good reason why ordinary users need Regedit, so I would enable
* 'Prevent Access to Registry editing tools'. Be careful with your logic here, the risk is that you have a double negative. For instance, 'Disable' the Prevent access to Registry, would allow Regedit to run, which may be the reverse of what you intended.

'Don't run specified Windows application', is another setting where you should double check your logic. Here you are making a list of the bad guys, programs that ordinary users have no business running.

'Run only allowed Windows programs', takes locking down the desktop one stage further, in this case you specify only programs that your people really need, for example, Excel and Winword. Remember that this is a list of a few essential programs.

* 'Restrict these Programs from being run from help'. This policy neatly closes a back door which savvy users exploit to sneakily run programs that they should not be using. Be on your guard, and choose the executables wisely.

Take a view on what should be done about 'Windows Automatic Updates'. Again, here is a policy to fit into your broader corporate network strategy.

Two settings which could slightly improve users experience are 'Configure Driver search locations' and 'Century Interpretation for year 2000'.The latter may be more relevant as we approach 2029!

* 'Code signing for drivers', this is not a setting that you should leave to chance, I would Enable, then 'Block' drivers without digital signatures. Ask yourself, 'What are users doing installing device drivers anyway?'.

User Profiles

I am a great fan of roaming profiles, especially for we administrators. With these settings you can alleviate worries that roaming profiles generate too much network traffic by imposing limits on the size of the profiles and the directories to include in the roaming profile.

Scripts

Nothing much here, perhaps you would want to run script visibly if you are testing, or if it had information for the users, but otherwise a section to ignore. By all means run legacy scripts hidden, but why not upgrade those Batch files to VBScript?

Ctrl Alt Del Options.

The most controversial decision here is the Task Manager (not Taskbar). My view is to leave it enabled. Would it not save work all round if users could zap their own programs which are not responding?

I can think of only a few specialist situations where you would want to deny users Change password, and Lock Workstations tabs. Kiosk computers or communal internet machines would benefit from this policy. However, for the rest, leave the Ctrl Alt Del as the default - not configured.

*Logon

There are two ideas here that are worth a look. Firstly, would there be any programs that clients always need? If so, then configure the 'Run Programs at Logon' setting. Secondly,

have you been caught by viruses exploiting the 'Run Once' registry setting? Well if so then you can block the registry RunOnce key with this policy.

Group Policy

* 'Group Policy Slow Link Detection', people often ask me what is a slow link? 56K, 256K? Well here you can decide, based on the experience of how long group policy settings take to apply when a client logs on remotely. The other settings here are to assist administrators who are configuring group policies.

Power Management

Just one policy here - Prompt for Password on Resume from Hibernate. This is the classic trade-off, security versus convenience. I do believe that hibernating rather turning machines off will be the way of the future. However, at present few people trust 'Hibernate' so this setting is not needed - yet!

Windows Time Service

If you are fed up with those Win32 Time errors in the Event Log then why not use a group policy to configure the Time Servers. In Windows Server 2003 domains Kerberos relies on time synchronization between servers, otherwise it thinks that a hacker has intercepted a packet and then put it back on the network 10 minutes later.