Global Information Assurance Certification Paper

GIAC Security Essentials Certification
Practical Assignment v 1.4, Option 1

Managing Security with Group Policy and the Windows Server 2003 Group Policy Management Console

Authored by: Norman Christopher-Knight
February, 2003

Table of Contents

Abstract

Group policy was first introduced with the release of Windows 2000 Server and Active Directory in the year 2000. With the introduction of Windows Server 2003, Microsoft has also released the Group Policy Management Console. The purpose of this paper is to highlight how this tool changes and, in most cases, improves upon the way that Group Policy is managed since the introduction of Windows 2000 and why it is important to security administrators and administrators in general. Additionally, examples will be provided to demonstrate how using this tool will enable to better control security and other related policies.

Chapter 1: Introduction and Group Policy Overview

I. Assumptions and Expectations

It is assumed that the reader has some experience with the issues involved in administering Windows server and client systems. More specifically, it is assumed that the reader is familiar with the concepts involved in using Active Directory and Group Policy.

Detailed explanations outside the scope of this paper will be referred to using Internet hyperlinks where possible. Details about specific Group Policy settings will only be given where it serves to illustrate a point of discussion. Refer to the references section for information about documents that will go into greater detail about the finer points of Group Policy.

Descriptions of other technologies will only be described in so far as they related to Group Policy or the management of Group Policy.

II. Introduction

Windows 2000 was released to the general public in February of the year 2000. Two of the most eagerly anticipated features of the new operating system, from a server perspective were Active Directory and Group Policy. Together, they held the promise of easing most of the suffering Windows Server NT administrators had to endure in managing their networks, especially in large enterprises.

Prior to Windows 2000, large Windows NT networks often had dozens or even hundred of domains in order to manage all the users, network resources, and administrative (read political) boundaries within their organizations. In contrast, with Active Directory, many of the same administrative goals could be accomplished using organizational units. This would eliminate the need for extra domains in most cases thus reducing the complexity of managing Windows based enterprises.

The use of organizational units provided an additional benefit. They could be used as a means of representing units of management for Group Policy, a way to distribute settings to workstations and server running Windows 2000 or later Microsoft operating systems throughout an organization.

III. Group Policy Overview

i. What is Group Policy?

In order to understand the significance of the Group Policy Management Console or any of the changes that it introduces, it is important to have some background information on Group Policy itself.

The simplest explanation of Group Policy is that it is a means of managing and configuring a group of Active Directory users and computers. However, that statement does not, of course, fully describe the technology.

Group policy supplants a previous Microsoft technology for managing groups of Windows 9x and Windows NT computers called System Policies. System Policies allowed you to control some desktop and security related settings on a user, group, or computer level. The settings were contained in a file named Config.pol if applied against a Windows 9.x based computer or NTconfig.pol if using Windows NT. Machines, upon start up and a user logon would look for the appropriate .POL file in the NETLOGON share of a domain controller and apply those settings. This all sounds quite good up to this point, but there were a number of limitations with the way System Policies worked.

1. There could really only be one policy, per platform, per domain. This was especially problematic for any computer policies (policies which modified settings specific to the computers themselves). There could only be one set of configurations that would apply to all computers running Windows 9.x or Windows NT. User profile specific configurations were not as troublesome as policies could be applied on the basis of group membership (referred to as group policies although they are not the same thing as in Windows 2000 Server and Windows Server 2003).
2. They only modified settings in the registry. Generally, either the HKEY_CURRENT_USER or HKEY_LOCAL_MACHINE settings depending on whether it was a user policy or computer policy. They could not do things like modify access control lists (ACL's) on Windows NT, set permissions in the registry, control group memberships, and other things involved with securing Windows computers.
3. Generally, Windows 9.x and NT machines would pull the policies from the domain controller that authenticated them. However, in the case of Windows 9.x machines and policies based upon group membership, they always looked to the primary domain

controller (PDC) for these settings.[1] This could be a problem if the computer was located over a slow wide area network link away from the physical location of the PDC. Logon times on these machines would be negatively affected.

4. System Policies were only applied upon startup and logon.[2] Once the user was logged in, even the applicable System Policy changed it would not get updated until the next time the user logged on. In many cases, users rarely log off during the course of a business day. In fact, there are many people who don't log off their computers at all unless something happens. This may be in spite of whatever corporate policies may be in place to attempting to govern this behavior.
5. Delegating control was difficult if not impossible with the System Policy model. Like many things in the Windows NT era, delegating administrative tasks meant being forced to "give away" much more than was needed.
6. Perhaps the most common criticism of System Policies was the fact that, even after the policies themselves were changed or removed, the settings they made to the registry remained. This is commonly referred to as "tattooing" the registry.[2]

As one may have surmised by now, the previous discussion of some of System Policies problems was leading up to a discussion of how Group Policies addresses and improves upon them. There are a number of ways.

1. Combined with Active Directory and, more specifically, organizational units (OUs), multiple group policies can be created and distributed throughout the Active Directory hierarchy. User and computers accounts can have more than one policy applicable to them based upon the site, domain, or OU they are in, security groups, or any combination.
2. In addition to being able to modify registry settings for both users and computers, group policy can also manage file system permissions, Internet Explorer settings, registry permissions, software distribution, etc. Also, there are hundreds of different settings that can be managed. Group Policy is also extensible by Microsoft or third parties so other pieces of software can potentially be managed with it as well.

---

[1] Sheesley, John "Understanding System Policies". Microsoft TechNet. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winntas/tips/techrep/systemp.asp. (February 8, 2004)

[2] Minasi, Mark. "Mastering Windows Server 2003". San Francisco: Sybex Inc., 2003. 737

3. Group Policies are replicated amongst domain controllers (DCs) and the policy is retrieved from the authenticating DC regardless of the settings within it. So long as the domain controllers are properly distributed taking WAN links into consideration, bottlenecks such as requiring the PDC emulator for certain settings should not be an issue.
4. Group Policy is applied to the user and computer accounts not only at startup and logon, but at periodic intervals (the default is 90 minutes) thereafter.
5. To counter perhaps the worst feature of System Policies, Group Policies do not tattoo the registry (unless custom ADM files are used). When the Group Policy no longer applies to a user or computer, the configuration changes that were made are reversed.
6. Control over Group Policies can easily be delegated to other people other than Domain or Enterprise Administrators without giving them access to everything else. Permissions can be provided to edit a Group Policy Object (GPO) that contains the settings to be deployed, but not to actually deploy them (by linking them to a site, domain, or OU).

ii. Group Policy Mechanisms Overview

Although administrators familiar with Windows 2000 Group Policy needed to use Active Directory Users and Computers to manage it, Group Policy is not only an Active Directory based service, but a file based service as well. There is one portion of a Group Policy Object (GPO) that is stored in the Active Directory and another that is stored in the file system

The Active Directory (AD) portion is called the Group Policy Container or GPC. This is the item that computers will query for to discover which policies are applicable to them upon boot up. AD permissions (for security filtering) and the object in AD that a GPO is linked to (a site, domain, or OU) determines what computer and user AD accounts Group Policy is applicable to.

Once the client determines which policies are applicable, the actual settings are stored in a series of files in the SYSVOL folder of AD domain controllers. SYSVOL is responsible for replicating file based data such as logon scripts amongst domain controllers. The file system portion of a GPO is known as the Group Policy Template or GPT. This section will not go into great detail about the GPC and GPT objects. Suffice it to say that it is important to be cognizant of the relationship

between the two when creating and modifying policies. If, for example, an administrator creates a GPO by using the AD tools, or even the GPMC but shortly thereafter, there is a problem replicating the SYSVOL data to other domain controllers, client machines will run into potential problems and will not be configured according to the administrators specifications.

The other thing to keep in mind is that GPOs are based in domains despite the fact they may be linked elsewhere. This is by nature of the fact that the AD and SYSVOL replication mechanisms they rely on are also defined by domain boundaries.

Another concept that should be understood is that of linking. It has been referred to a couple of times already at this juncture. What it is referring to is the ability to connect or assign a GPO to an AD object. The objects that GPOs can be linked to are sites, domains, or organizational units (OUs). Various policies can then be applied to different users and computers based upon their position within AD. For example, if a company has a domain divided into various organization units, then user accounts in some OUs can get different policies applied to them depending on what OU they may be in. There are many different ways of deciding upon how to divide certain groups of computers or users into OUs. Some reasons could be political, geographical, or technical.

Chapter 2: Group Policy Management Console Overview

The Group Policy Management Console (GPMC) was designed to address shortcomings with the way Group Policy was managed in Windows 2000 without forcing businesses to purchase potentially third party utilities. It is very important to realize that the GPMC does not in any way, shape, or form, change the underlying mechanisms by which Group Policy works. Rather, it changes the way administrators create and interact with the Group Policy objects in the Active Directory. For example, a Group Policy object can be created using either the GPMC or the default tools in Windows 2000 or 2003 but edited and managed using the other.

The GPMC is not included on the Windows Server 2003 CD but was made available as a free download from Microsoft's website shortly after 2003's April 24th, 2003 release to the general public. The most recent version, the GPMC with Service Pack 1, is available on the Windows Server 2003 Feature Pack page. Follow the link below to get to the Feature Packs page and then select the Group Policy Management Console link to go to the download page for that tool:

http://www.microsoft.com/windowsserver2003/downloads/featurepacks/default.mspx

I. Managing Group Policy Prior to the GPMC

Prior to the introduction of the GPMC, several tools were required in order to properly manage Group Policy. In some cases, no specific tool (at least from Microsoft) was provided at all and special "tricks" were needed in order to fill the gaps.

The way Group Policy is managed in a Windows Server 2003 without the GPMC installed is exactly the way it was managed in Windows 2000 Server with the exception of an additional tab

So what specifically were the problems with managing group policies in Windows 2000? That must first start with an understanding of how they were managed in the first place.

i. Group Policy Processing Order

It is pivotal, before even creating the first Group Policy object (GPO) in a forest, that the way in which they are processed is understood. Failing to understand this can have far reaching consequences in a distributed environment such as Active Directory. This is especially true of medium to large enterprises that will have complex directory hierarchies based on any combination of political, geographical, administrative or other organizational boundaries.

As almost any text on Group Policy will tell you, remembering the following acronym will make remembering the processing order itself much easier. It is **LSDOU**. The following describes each item in more detail:

- **Local Computer Policy:** As mentioned earlier, each Windows 2000, Windows XP, or Windows Server 2003 computer has a local Group Policy object which has many settings in common with Group Policies linked to objects in the domain. Any of the aforementioned Windows operating systems will process this first before beginning to process any policies set in the Active Directory.
- **Sites:** Once the Local Computer Policy is processed, then Active Directory based Group Policy objects are processed starting with any object linked to the AD site of which the computer is a member.
- **Domains:** Any policies which are linked at a domain level are dealt with next. If the user account happens to reside in one domain and the computer they are logging into another, any applicable policies from both domains will be applied to the user and computer respectively. The domain level is the only place where important settings such as account policies are set for users.
- **Organizational Units:** Finally, any organizational units which contain the user account logging on or the computer account for the machine being logged on to have their GPOs processed last. Organizational Units allow for great control over what user and machine accounts apply group policy and don't and allow for easy delegation of authority in managing GPOs.

The significance of knowing the order in which GPOs are processed is that it tells us which GPOs settings will take precedence in the event of setting conflicts. Normally a machine and user account will process any applicable GPOs in the AD hierarchy. So if there are GPOs set at the site, domain, and organizational unit, they will be processed even if accounts are in a sub-OU that does not explicitly have a GPO linked to

it. This behavior is consistent with the way permissions themselves are inherited by objects in AD.

A setting conflict is when there are two or more GPOs processed and each of them has one more of the same items set in the policy. For example, if a domain policy sets permissions on the Server service for Windows workstations and servers such that members of the Domain Admins group have permissions to stop and start that service while another policy linked to a lower level OU sets it so that only the Enterprise Administrators group can stop or start the Server service, then Domain Admins will not be granted the permissions when logging on to machines whose accounts are in that OU.

The bottom line is that any policies processed last will win in a conflict resolution scenario. It should be noted that GPO links higher in the list of an object (such as an OU) have higher precedence than other GPOs linked to the object. They too will "win" in the event of setting conflicts.

ii. Creating or Adding Group Policy Objects in Windows 2000

With the order of processing GPOs in mind, we can then turn our attention to how to create and link the objects at the site, domain, or OU levels. The process and interface is essentially the same amongst all three levels. The only difference is that, for sites, the **Active Directory Sites and Services** tool is use whereas for domains and organization units, **Active Directory Users and Computers** is used instead.

One can mitigate the inefficiency of having to use two separate tools in order to see all the necessary GPO links by creating an MMC console that contains both AD Users and Computers and other tools that they may use on a regular basis.

To create a new GPO and immediately link to an AD site object, the steps are as follows:

1. Launch **Active Directory Sites and Services**. Expand the **Sites** node and then right click the desired site.
2. From the resulting context menu, select **Properties** and go to the **Group Policy** tab.

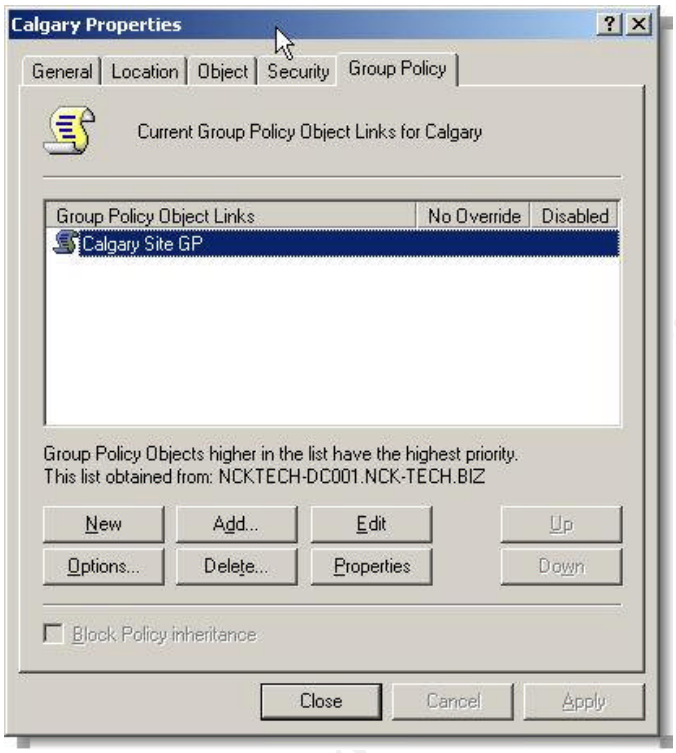

Figure 1: An example of a Windows 2000 style Group Policy object linked to the Calgary site. This properties window is where a number GPO related task would be initiated.

3. Click on the "**New"** button. An item named **New Group Policy Object** will appear under the **Group Policy Object Links** column. It can immediately be renamed.
4. To edit the GPO's settings, double click it or highlight it and click the **Edit** button.

The process above creates a brand new GPO and immediately links it to the site OU. If there is already an existing GPO in AD, then it can simply be linked to the site following a similar process above. The only difference is in step 3 where the **Add** button would be used. This will open the **Add a Group Policy Object Link** windows pictured below.

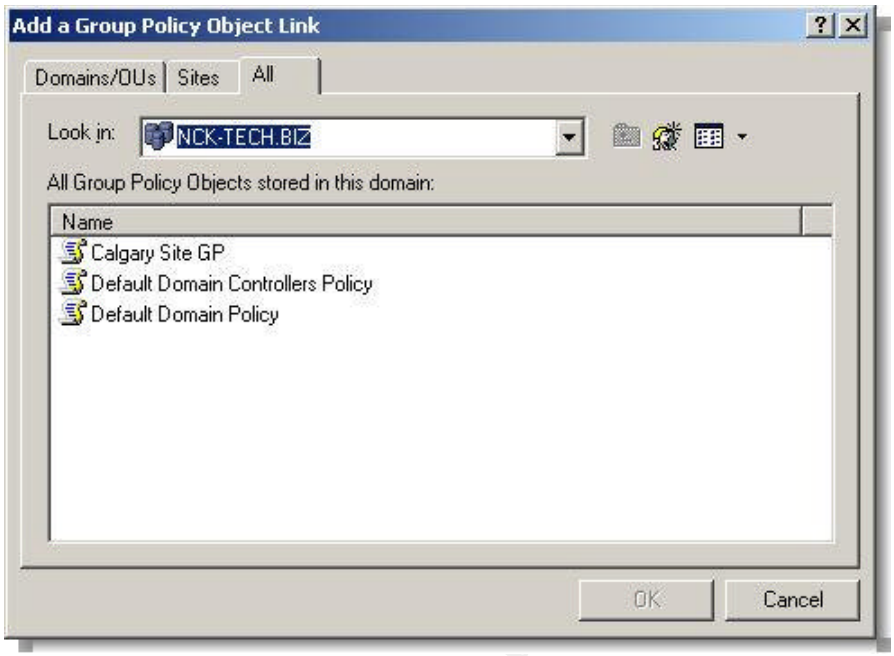

Figure 2: The **Add a Group Policy Object Link** window. It was previously the only way to see all GPOs for multiple domains in one place. The first two tabs show GPOs linked to domains, OUs, or sites, the **All** tab shows all GPOs, regardless of whether or not they are linked to any AD objects.

The intended GPO can be selected from one of the three tabs pictured above. The **Domains/OUs** tab will allow you to select GPOs linked to a domain or OU within a domain. You can select the specific domain, if there is more than one, from a drop down list box on the tab.

The **Sites** tab organizes GPOs based on which AD site they are linked to. Again, the specific sites can be selected from a drop down list box. Finally, the **All** tab allows you to see all GPOs in a domain regardless of whether or not they are linked to any AD objects. It is the only GUI based method of seeing unlinked GPOs.

With respect to creating or adding GPOs to domains or OUs, the interface is the same as that described for sites. The only difference, of course, is going into the properties of the domain or OU object in **Active Directory Users & Computers** and going to the Group Policy tab.

iii. Performing Additional Group Policy Object Tasks in Windows 2000

Referring back to Figure 1, there are other tasks that can be performed on GPOs and GPO links using the Group Policy tab.

1. **<u>The Options Button</u>:** This button exposes properties that can be enabled on a GPO link.
    a. **No Override:** With this option set, the settings in the applicable GPO will be enforced on OUs lower in the AD hierarchy regardless of whether or not they have the Block policy inheritance option (described later) set.
    b. **Disabled:** With this set, the applicable GPO will not be applied to user or computer objects which would otherwise be governed by it. Furthermore, any computers that previously had settings based on it will remove them on the next Group Policy update cycle.[3]

Figure 3: An example of the options available on a GPO link. No Override will enforce the GPO settings on lower OUs and Disabled will render a GPO link not applicable to user and computer accounts to which it normally would be.

2. **<u>The Delete Button</u>:** This button offers you two options.
    a. **Remove the link from the list:** The default, this will remove the item from the Group Policy Object Links column but it will still exist in the domain should you need to link it elsewhere. You would have to use the Add button and go the All tab in order to see the unlinked GPO (as described earlier).
    b. **Remove the link and delete the Group Policy Object permanently:** Your other option is to delete the GPO link and the GPO itself. If there are no plans to ever use the GPO again, it would be wise to use this option.

[3] Mar-Elia, Darren. "The Definitive Guide to Windows 2000 Group Policy". RealTimePublishers.com. 2001. 62

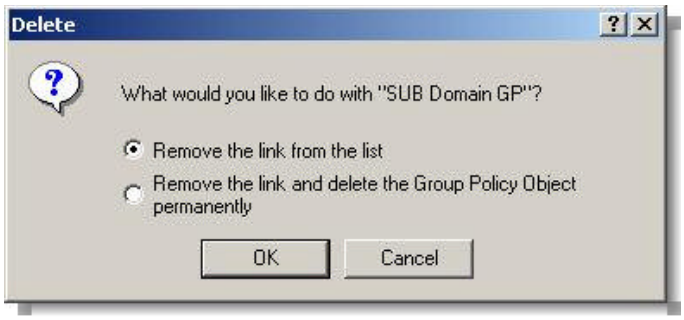

Figure 4: The options presented when clicking on the Delete button. You can either remove the link from the site, domain, or OU leaving the GPO intact and available for later use or delete both the link and the GPO itself.

3. **The Properties Button:** This item allows you to manipulate the properties of the actual GPO itself rather than just the link.
    a. **The General Tab:** On this tab of the GPO Properties window, there are a couple of options: **Disable Computer Configuration Settings** or **Disable User Configuration Settings.** Checking either of the two boxes off will cause computers processing the GPO ignore the computer or user portions of the policy respectively? This can be an improvement in performance as computer will not have to even attempt to enumerate all the settings within that portion.

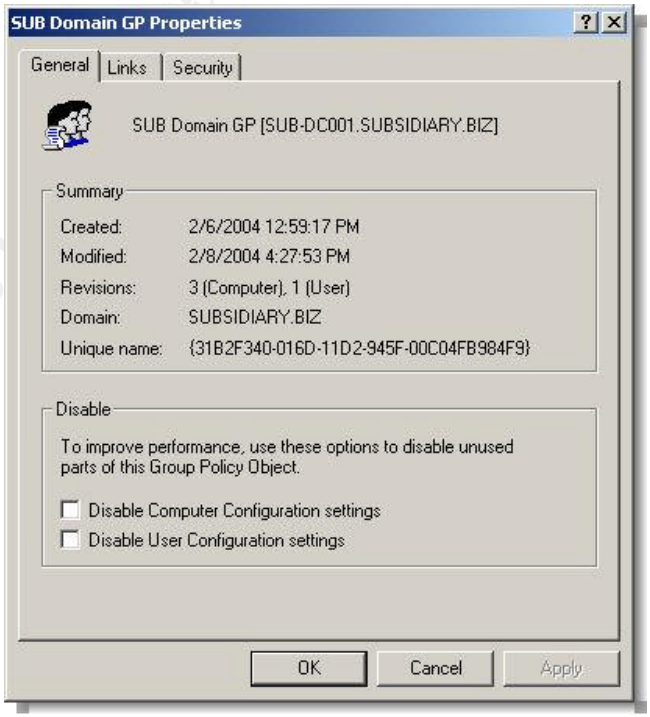

Figure 5: The General tab of the Properties window on an example GPO. From here, either the computer or user portions of the GPO can be disabled to improve processing performance.

b. **The Links Tab:** Using this tab, a search can be performed for all the places that the GPO is linked be they sites, domains, or OUs.

Figure 6: The Links tab of the Properties window on an example GPO. All sites, domains, or OUs to which the GPO is linked can be searched for and revealed here.

c. **The Security Tab:** Rights that can be assigned to the GPO object itself in Active Directory can be set here. GPO filtering is often done using this tab. By removing the default of the Authenticated Users group and using other, more specific security groups, the GPO can be filtered so that only specific portions of users or computers within a site, domain, or OU will process the policy. A user or computers account must have at least both Read and the Apply Group Policy rights in order process a GPO.

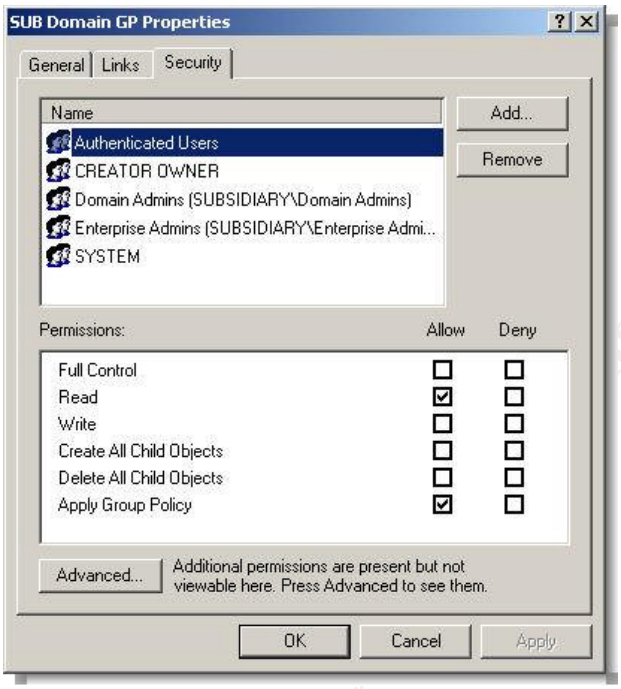

Figure 7: The Security tab of a GPO. The most common use of this tab would be to set the permissions so that the GPO could be filtered on the basis of user or computer group memberships.

d. **The Edit Tab:** Using this button yields the same result as double clicking the GPO link. It opens the Group Policy Object Editor and allows you to directly edit the settings of the GPO.

II. Difficulties Managing Group Policy Prior to the GPMC

With an understanding of how Group Policy is managed in Windows 2000 environments (or Windows Server 2003 environments without the GPMC), one can start to better comprehend the short comings as well.

i. No All Encompassing Group Policy Management Tool

While it is true that the majority of Group Policy tasks could be carried out from Active Directory Users and Computers, it is also true that multiple tools needed to be used in order to manage all aspects of Group Policy. The most obvious example is the fact that Active Directory Sites and Services need to be used in Windows 2000 environments in order to link GPOs to sites and manage them.

Another major issue pertaining to the lack of a single management tool is that it is very difficult to determine all of the applicable GPOs impacting the settings that are applied to users and computers. For example, machine and user accounts nested in OUs low in the AD hierarchy may have other GPOs in parent OUs or at the domain or site level that they are receiving settings from. However, AD Users and Computers and the Sites and Services tool only let you see the GPOs that are linked to a site, domain, or OU one at a time.

ii. No Ability to Produce Reports of GPO Settings

The only way without the GPMC to view the settings of a particular GPO is to use the Group Policy Object Editor and manually scan through the nodes to see which items are set. There is somewhat of a limited capability to show only configured items in the nodes under Administrative Templates but this is not the case with other settings, most notably security settings in the computer portion of the GPO itself.

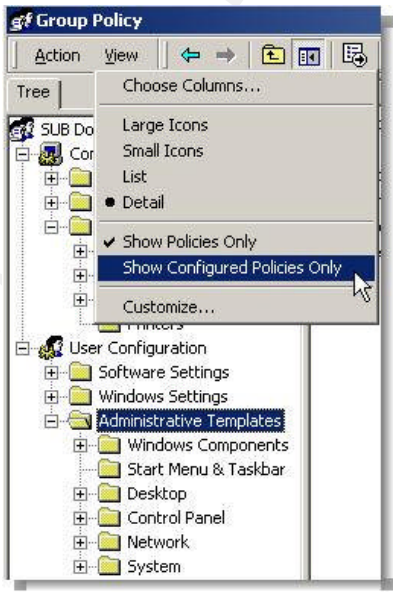

Figure 8: The Group Policy Object Editor option to show only configured policies. This option is only valid for settings under Administrative Templates.

This especially vexing limitation when you take into account that, without Edit permissions on the GPO, the settings cannot be viewed using the Group Policy Object Editor. In many medium to large organizations, there will undoubtedly be differing levels of administrators each responsible for different portions of the AD hierarchy. Naturally, administrators of higher level OUs or the domain and site levels will want to limit who can edit or otherwise modify their GPOs. That said,

administrators of lower level OUs still need to understand where settings are being inherited from in addition to any they may have set themselves. In the Windows 2000 model, at best, they would have to rely on any documentation produced by higher level administrators that is if any had been produced at all.

iii. No Backup, Restore, Capabilities and Limited Import-Export Capabilities

One very glaring omission from the Group Policy toolset prior to the GPMC is the lack of a comprehensive backup and restoration tool for GPOs. In a limited fashion, this can be accomplished by backing up the SYSVOL portion of a GPO and then manually moving files around but this far from a reliable and easy to manage method.

There is also, no easy method of importing settings into an existing GPO. The one exception to this, and very important from a security perspective, is the Security Settings portion of the computer policy. As depicted in Figure 9, by right clicking on the Security Settings node, a security template can be imported. Thus administrators can create security templates and, once satisfied with their contents, import them into the Security Settings node. In the event of the loss of the GPO, a new one can be created and the security settings imported back in.

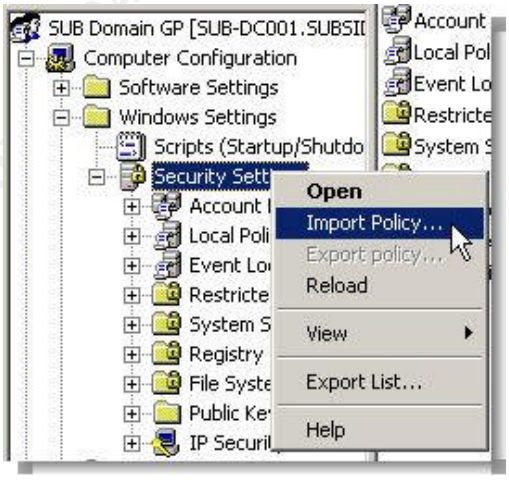

Figure 9: The one exception to the lack of an import tool for Group Policy objects. The security portion of the computer part of a GPO can import from security templates.

Unfortunately, none of the other portions of the GPO can benefit from the ability to import or export settings with the standard Windows 2000 and 2003 tools.

iv. No Tool for Moving GPOs between Domains

Closely related to the previous problem is the fact that GPOs cannot be easily moved between domains. Despite the fact that they can be linked almost anywhere in an AD forest, GPOs are bound to the domain in which they were created. GPOs benefit from AD replication to distribute themselves to other domain controllers. Both at the AD database level and at the file system level (through replication by the File Replication Service of the SYSVOL share).

There are especially difficult problems when attempting to move GPOs between two or more untrusted domains. There are legitimate reasons for wanting to do this. Perhaps the most common would be moving from a testing or lab environment into production. Often, especially in larger networked environments, GPOs are tested in a lab, isolated from the production network to avoid any potential problems. Ideally, once this testing was completed, rather than manually duplicating all the settings in a GPO by creating a brand new one in the production AD, the test GPO could be moved to production. This is assuming that only minimal "tweaking" would be required compared to recreating it from scratch.

v. The Bottom Line: No Easy Way to Determine the Resultant Set of Policy

Looking back at the problems listed above, most of them boil down to one major problem. The Windows 2000 model of managing Group Policy has no easy way of determining the full scope of what is going on. There isn't an easy way to determine all of the settings from GPOs distributed throughout Active Directory and impacting the final configuration of a computer and the user logged into it.

The settings in effect for computer and user objects after all policy objects have been processed are, in Microsoft parlance, often referred to as the Resultant Set of Policy or RSoP. Since so many factors contribute to what GPO settings finally get applied to a machine and a user logged on to it, there needs to be way to easily identify what settings are in effect on a machine and where the "winning" settings came from.

III. Enter the Group Policy Management Console: Addressing the Problems

The Group Policy Management Console (GPMC) eliminates or eases a number of these concerns. Specifically, the GPMC brings the following features to the table.

1. **Single GUI Interface for Managing Group Policy:** Essentially all aspects of Group Policy management have been unified somewhere in the GPMC interface. Some examples include:
    a. Creating and editing GPOs.
    b. Linking GPOs to sites, domains, or OUs.
    c. Backing up and importing GPOs
    d. Managing GPOs and their links across domains both trusted and untrusted.
    e. Delegating permissions on GPOs such as being able to edit them or link them to containers.
    f. Determining the resultant set of policy (using functionality built into Windows XP and Windows Server 2003).
2. **Reporting of GPO Settings and Resultant Set of Policy (RSoP) Data:** The GPMC can produce HTML based reports on the settings within a GPO or from actual or simulated RSoP data. These reports can be saved, printed, e-mailed, etc. The reporting function overcomes the limitation of the GPO Editor in that one only needs Read permissions on the GPO to product a report and see the settings it contains. Recall with the GPO Editor, if you do not have Edit permissions on the GPO, it will not open.
3. **Backup, Restore, and Import Capabilities:** The GPMC provides an easy way of backing up GPOs so that they can be restored if a disaster occurs, or settings from backed up GPOs can be imported into others.
4. **Moving GPOs between Domains and Forests:** The GPMC, using the various mechanisms discussed briefly in item 3 above, can be used to move GPOs across domains, even into different Active Directory forests.
5. **Determining the Resultant Set of Policy:** Arguably the most useful feature of the GPMC is the ability to leverage the functionality built into Windows XP and Windows 2003 to determine the RSoP for a given computer and user combination. Furthermore, the tool can actually give data that shows all of the settings that would have been applied, plus the GPO that set each of settings. Referred to as the Winning GPO in the Microsoft literature.

One thing that is important to note. The GPMC can be used to manage both Windows 2000 and Windows 2003 Group Policies. The only caveat is that it cannot be installed directly onto a Windows 2000 Professional or Server installation. Only Windows XP with SP1 and Windows Server 2003 are supported.

i. The GPMC Interface

The GPMC addresses a previous concern that there was no “one stop” tool that could be used to manage the numerous aspects of Group Policy. Figure 10 below shows a typical view of the GPMC MMC interface. Although it does not capture all aspects of the tool in a single screen shot, there are a number of things of note. Details on how to use the tools are in the next chapter.

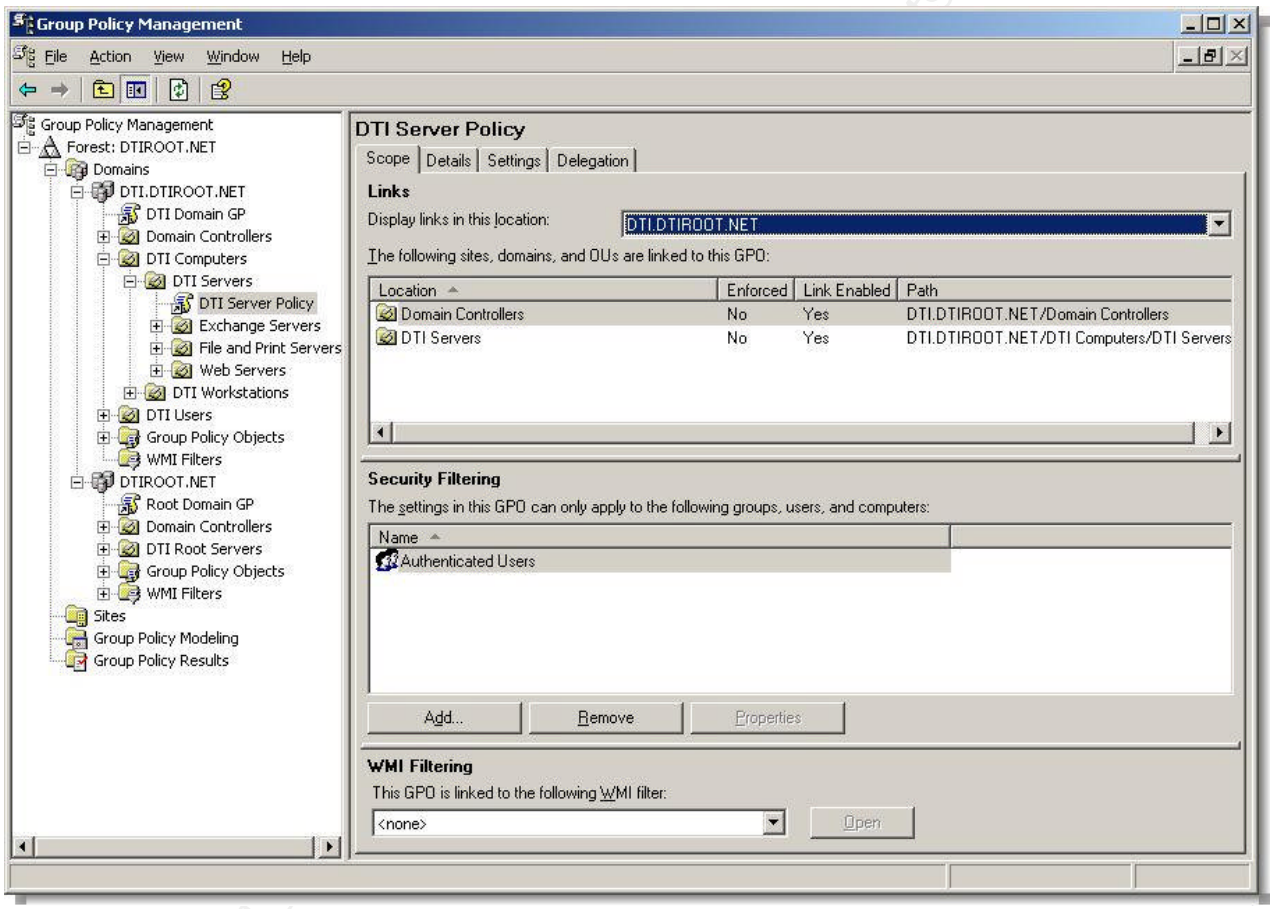

Figure 10: Typical view of the Group Policy Management Console. The left pane of the MMC snap in shows forests, domains, OUs, and the GPOs linked to them. Sites themselves are also visible as well as the Group Policy modeling and results objects. The right hand pane shows some of the settings that can be set on the DTI Domain GP GPO link.

The GPMC is an MMC snap-in which means it shares many of the characteristics of most snap-ins. The left hand pane offers a tree like view of the manageable objects within the tool. In this case, the tree view is very similar to the one found in Active Directory Users and Computers. It essentially shows Active Directory forest hierarchies starting with the forest level and showing the domains within each forest. The domains expand further into OUs. Finally, the leaf objects

underneath those are the GPO links associated with them. In an effort to more easily distinguish between links and GPOs themselves, the icons for the links are similar to normal Windows Explorer shortcuts with a small arrow in the lower left hand portion.

Sites are displayed at the same level as domains in the GPMC. Expanding the site object will reveal a view similar to that of the domains in that the GPOs linked to the site will be revealed.

The final two objects are Group Policy Modeling and Group Policy Results. Group Policy Modeling will not even appear if the Active Directory does not have the Windows Server 2003 schema extensions and at least one domain controller running Windows 2003. As the name implies, this tool can be used for planning purposes. Once you have created a GPO, you can run simulations changing variables such as the user and computer accounts used, what group memberships they have, where in the Active Directory hierarchy they are, etc. You can see what the RSoP would be without actually having to make any changes in production.

Group Policy Results is used for determining the RSoP information from the *actual* set of policies that was applied to a computer and (if required) a user logged on to the machine.[4]

The right hand pane, in typical MMC snap-in fashion, will display management options contextually relevant to the object highlighted in the left hand pane. In Figure 10, the object highlighted is the DTI Server Policy GPO link. The items displayed are the following:

1. **The Scope Tab:** This is a single view that will display all the places in AD where the specific GPO is linked and who the policy will be applied to.
2. **The Details Tab:** This tab provides very specific information about the GPO itself. Information includes the domain in which it resides, version numbers, and its globally unique ID or GUID.
3. **The Settings Tab:** Is undoubtedly one of the most useful tools in the GPMC. It displays a report of all the *configured* settings within the GPO in HTML format. Individual portions of the policy (such as the Security Settings or Internet Explorer Maintenance)

[4] Lundy, Jim. "Administering Group Policy with Group Policy Management Console". Group Policy Results. April, 2003
URL: http://download.microsoft.com/download/a/9/c/a9c0f2b8-4803-4d63-8c32-3040d76aa98d/GPMC_Administering.doc (February 3rd, 2004)

can be expanded or hidden. Reports can be printed, saved, e-mailed, etc.

4. **The Delegation Tab:** This provides a simple interface for delegating permissions on the GPO. For most things, simple "role" based permissions are available (such as Edit or Read). If more granular permissions are needed, the Windows ACL Editor can be launched.

There, of course other options that are displayed depending on the context of the object displayed in the left hand "tree" pane. These, in addition to the items detailed above, will be covered in greater detail in Chapter 3.

ii. The Relevance of the GPMC from a Security Perspective

Although, in the minds of many security professionals, the relevance of Group Policy and its management may be obvious, it is nonetheless worthwhile to specifically state its value.

Group Policy, in the modern Windows world (Windows 2000, Windows XP, Windows 2003), is the configuration tool of choice for a variety of settings and configurations not the least of which are security related. Why is it the tool of choice? It provides the ability to manage settings for multiple users and computers automatically reducing or eliminating the need for individually configuring computers and user profiles. As a result, the possibility of omissions or errors is also reduced. In a word, *consistency* can be more easily achieved.

Consistent configuration is a vital component in any secure networked environment. The IT department may have done their due diligence in terms of determining what software installations, values, etc. are required in their environment to ensure a reasonable level of security, but a single mistake in configuring a computer can be the springboard to other problems down the road. Especially in light of the types of security vulnerabilities that are being reported today. For example, in August, 2003, the MS Blaster worm propagated by scanning and infecting machines over the network. A single infected laptop was often all that was needed to begin a chain of infections that would ultimately bring an entire network to its knees. While there is no known exploit yet, the vulnerability described in Microsoft Security Bulletin MS04-07 ASN .1 Vulnerability Could Allow Code Execution (828028). This is a vulnerability that can allow an attacker to remotely execute commands and take over a machine. What's more, unlike the MS03-026 vulnerability, there are multiple ports and other "attack vectors" that can be exploited.

Managing and security networked machines is often a complex proposition, even if the network only consists of a dozen machines. Considering the hundreds of settings that Group Policy can handle coupled with the potential for interacting with other policies, naturally, Group Policy can itself be very complex. Any tools that can help provide clarity when planning and deploying policies will ultimately allow administrators do to an even better job of securing machines. In some cases, those who may not have attempted to use policies extensively may now be tempted to do so.

Chapter 3: Using the Group Policy Management Console

This chapter will provide more specific detail on using the GPMC to carry out common tasks. In many instances, these tasks were done using other tools or not at all if there was no tool to do so previously.

The Group Policy Management Console (GPMC) is not part of the "gold" or original release code for Windows Server 2003. Microsoft took a different approach with several components of Windows Server 2003 including the GPMC. Rather than delay the public release of Windows Server 2003 in April, 2003, Microsoft instead decided to offer certain features or components using an "out-of-band release strategy".[5] The term simply means that Microsoft would break from its usual approach of waiting until all the pieces of an operating system were ready before releasing it and would instead add them later on after the products release.

In addition to the GPMC, some other products that are available on Windows Server 2003's Feature Packs page as free downloads are:

- Automated Deployment Services: A new service that allows administrators to create images of their servers and deploy them onto multiple servers that have absolutely no previous software on them concurrently.
- Windows Rights Management Services: A server service that works in conjunction with rights enabled software such as Office 2003 to allow organizations to control what can be done with documents with a much finer degree of control than simply file permissions. For example, with this service, you can restrict who can forward documents or e-mails, print them, etc.
- Active Directory Application Mode: This is an implementation of Active Directory that allows software developers the ability to use a directory to store information such as user and other permissions information in a replicable directory, but not directly in the corporate Active Directory running on domain controllers. It can however leverage the security in the domain based Active Directory security principals.

[5] Otey, Michael. "Windows 2003: An Out of Band Experience" Windows & .NET Magazine September 2003. http://www.winnetmag.com/Article/ArticleID/39778/39778.html (February 7th, 2004)

I. Installing the Group Policy Management Console

i. Installation Requirements

The GPMC can only be installed on the operating systems as shown in the table below.

Operating System	Service Packs and Hotfixes	Additional Software Requirements
Windows XP Professional	Service Pack 1 or Service Pack 1a and the Hotfix described in Microsoft Knowledge Base article 326469.	Microsoft .NET Framework
Windows Server 2003		

Table 1: Summary of the installation requirements for installing the GPMC.

As you can see, installation on Windows XP has some additional requirements that aren't necessary on Windows Server 2003. For example, the .NET Framework must be installed on Windows XP Professional because it does not come with it like 2003 does.

Administrators would most likely install the GPMC on a Windows XP workstation so that they would not have to log on to a Windows 2003 based server each time they wanted to administer Group Policy.

Windows XP Professional and 2003 support special functionality for determining the Resultant Set of Policy (RSoP) applied to a computer and (optionally) the logged in user. The GPMC leverages these services which is an additional reason why GPMC requires Microsoft's latest desktop and server operating systems.

The remainder of this description will focus on installing GPMC on a Windows XP Professional machine. Most of the steps can be omitted for installation on Windows 2003 with the exception, of course, of running GPMC.msi, the installation file itself.

ii. Downloading the Group Policy Management Console and the .NET Framework

The GPMC as well as other feature packs can be downloaded from Microsoft's Windows 2003 Feature Packs page at the URL below:

http://www.microsoft.com/windowsserver2003/downloads/featurepacks/default.mspx

Click on the Group Policy Management Console link to download the GPMC. The latest version is the Group Policy Management Console with Service Pack 1 which includes code fixes, additional language support, and a new end user license agreement (EULA).

Save it locally on the hard disk or a network share. Do not attempt to install it yet. Next, the .NET Framework will be installed (assuming it isn't already) from Windows Update.

Go to Windows Update and install the .NET Framework 1.1 as follows:

1. Open Internet Explorer and launch Windows Update from **Tools\Windows Update**.
2. In the right hand pane click **"Scan for updates"**. Once the scan is complete, click on **"Windows XP"** link in the left hand pane.
3. If the installation of Windows XP was not done using SP1 slipstreamed media, go to the **Critical Updates and Service Packs** option and SP1 to be installed.

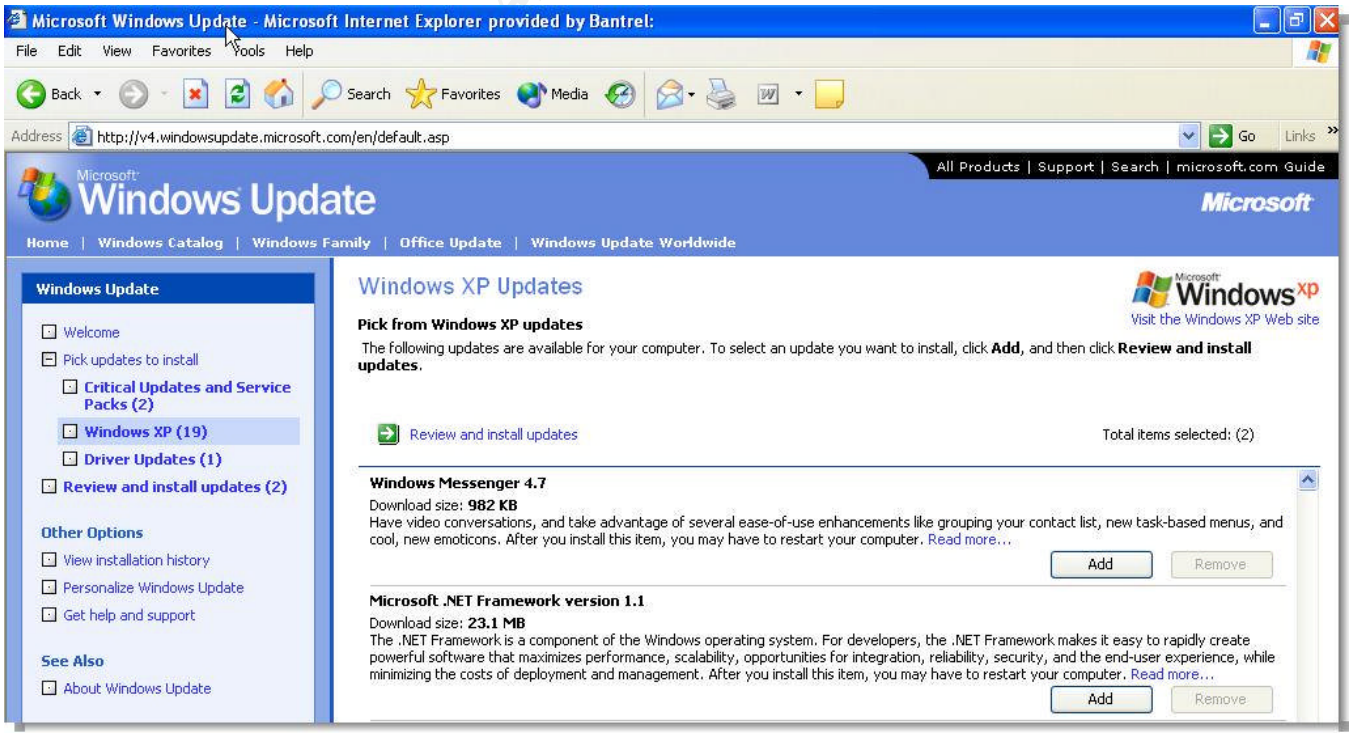

Figure 11: The Windows XP Updates page from Windows Update. The option to install the .NET Framework 1.1 is shown.

4. In the right hand pane under Windows XP Updates, click **"Add"** button beside the **"Microsoft .NET Framework version 1.1"** option. Then click on the **"Review and install updates"** link.
5. The view in the right hand pane will change to say "Total Selected Updates". Click on the **"Update Now"** button to begin the installation process.
6. If you installed SP1 or possibly other installations, you may have to reboot the machine. Click **"OK"** if prompted to do so.

iii. Running the Group Policy Management Console Installation

Now that the prerequisite software has been loaded, the GPMC itself can be installed.

1. Navigate to where you saved the GPMC.msi file that was downloaded and double click it to start the installation.
2. Click **"Next"** when the first page of the installation wizard appears. On the License Agreement page click on the **"I Agree"** radial button and then click **"Next"**.
3. The dialog box pictured in Figure 12 below will appear indicating that the MS KB hotfix Q326469 needs to be installed (because the installation detects it is running on Windows XP). Click **"OK"** and then click **"Next"** when the install wizard for the hotfix itself appears.

Figure 12: Prompt during the GPMC setup to install QFE Q326469 hotfix when installing on Windows XP.

4. On the License Agreement page for the hotfix, select the **"I Agree"** radial button and then click **"Next"**. The installation will create a restore point and install a new version of GPedit.dll (version 5.1.2600.1186).
5. Click **"Finish"** once the hotfix itself has been installed. This immediately returns to GPMC installation and allows it to finish.
6. Click **"Finish"** once the GPMC installation completes.

Once the GPMC has been installed, it can be launched from **Start\Programs\Administrative Tools\Group Policy Management** or by running GPMC.msc from the Run dialog box or a command line.

An even better option is to add the GPMC snap-in to a custom MMC console along with other tools that would be beneficial such as Active Directory Users and Computers, Computer Management, etc.

II. Configuring the Group Policy Management Console

With the GPMC, Group Policy in multiple forests and domains can managed from a single console. That said; it is prudent to set up the GPMC snap-in so that all of the forests and domains that need to be managed are immediately available.

Also, the GPMC has a set of Options that can affect what you can and cannot add to the GPMC. This will be discussed in the following sections.

i. The Group Policy Management Console User Interface Options

The User Interface Options (hereinafter referred to simply as Options) in the GPMC allow you to configure the columns that appear given the context that you are in, the location that the GPMC searches for ADM files (more on this later), and some other general options that will be detailed below.

To expose the Options window, open the GPMC MMC and click on the **"View\Options"** menu. The window pictured in Figure 13 will appear.

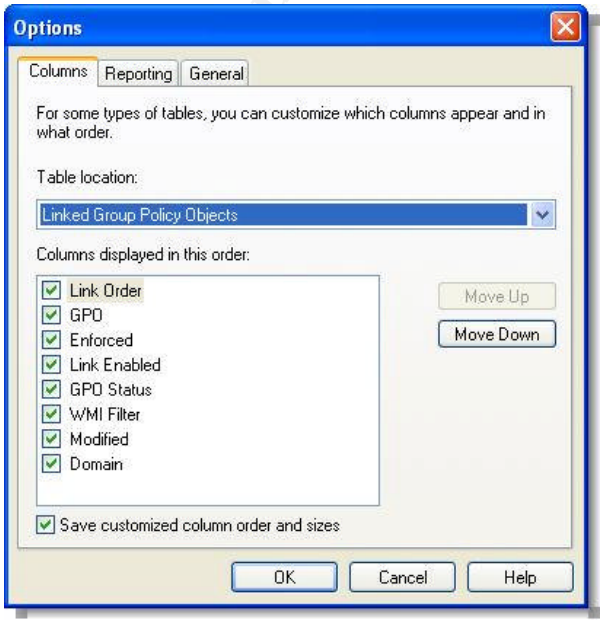

Figure 13: The initial view seen when opening the GPMC User Interface Options window.

It will have three tabs as pictured. They are described next.

1. **The General Tab:** Pictured in Figure 13, this tab allows you to set the columns that will appear in the right hand side of the tool given the object highlighted in the left hand column. You can select the type of table you wish to configure using the drop down list box. The available columns will change based upon what has been selected. The columns can be turned on or off and reordered for:
    a. **Group Policy inheritance:** This tab which appears when a site, domain, or OU is selected in the left hand pane of the GPMC, shows all the GPOs that settings will be inherited from. In the case of domains, and OUs, this list does not include any GPOs linked at the site level.
    b. Group Policy objects: When the Group Policy Objects container is highlighted, this is where the columns displayed can be selected.
    c. Linked Group Policy objects: This tab which appears when a site, domain, or OU is selected in the left hand pane of the GPMC shows all the GPOs directly linked to the object. The columns that are displayed can be chosen here.
    d. WMI Filters: This node is only displayed in domains with the Windows Server 2003 schema and at least one DC running Windows 2003. The columns that appear when this node is highlighted can be selected here.

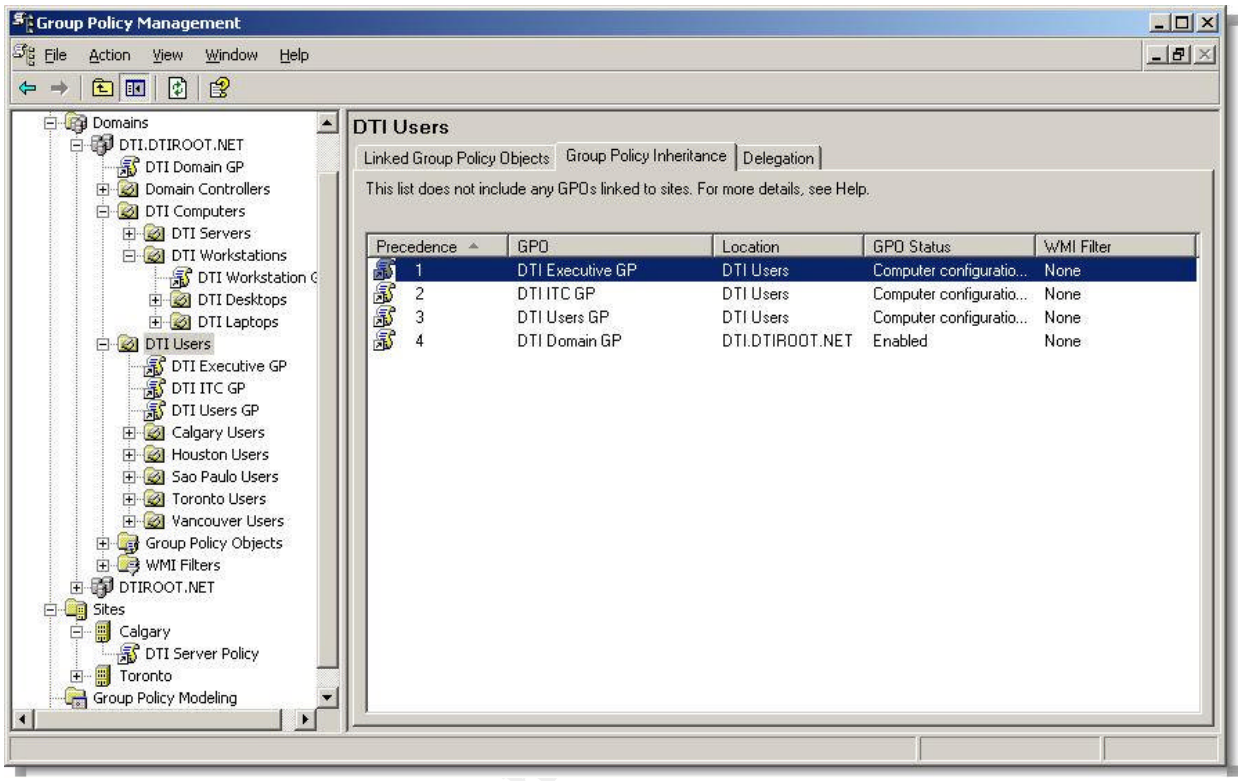

Figure 14: Displaying the 3 tabs displayed when highlighting a site, domain, or OU object in the left hand pane. Relevant to the discussion above are Linked Group Policy Objects and Group Policy Inheritance (pictured above)

2. **The Reporting Tab:** In order for the GPMC to display its reports, it must be able to find the appropriate ADM files for Group Policy Administrative Templates. The default behavior is to search Windows folder on the local machine and then the SYSVOL folder on a domain controller.

   The purpose of this tab then is to allow a user to override the default behavior and specify and location that they want their tool to look in always before the default locations.

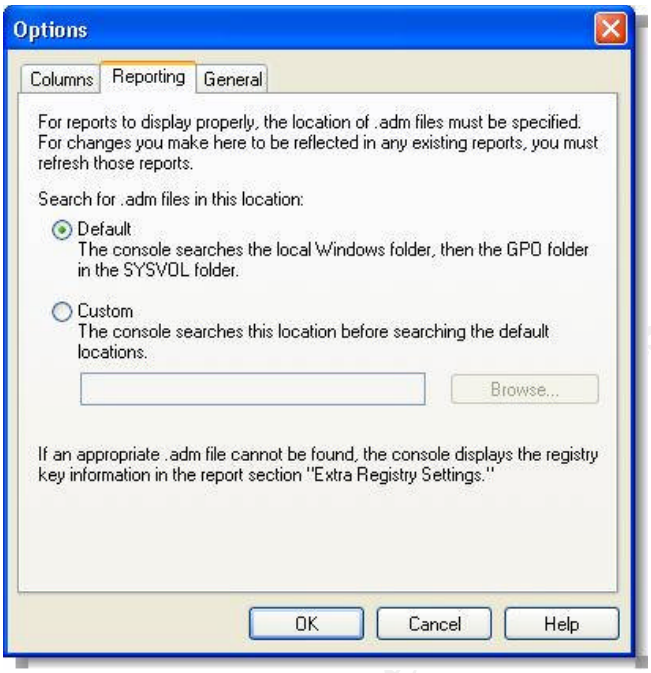

Figure 15: The Reporting tab for the User Interface Options. Allows you to set a custom location for ADM files needed to generate reports.

3. **<u>The General Tab</u>:** The options set on this tab will govern what forests can be added to the GPMC, and some other interface options.
    a. **Trust Detection:** The default installation of the GPMC will only allow the addition of a forest in which there is a two way trust with another forest. For the purpose of the examples in this paper, this will be turned off so that an un-trusted forest can be added. This would also be necessary in the case of a 1 way trust situation.
    b. **Show Domain Controllers after Domain Names:** This option allows you to specify whether or not the GPMC will display the domain controller being used to retrieve data from for a given domain. It is most likely a good idea to leave this setting on as it will make you aware of which domain controller you are editing your GPOs on. This is useful when troubleshooting situations in which settings were not applied due to replication issues, etc.
    c. **Show confirmation dialog to distinguish between GPOs and GPO links:** The default after installation is to have this option on. Each time you click a GPO link, you will be prompted to make you aware of what you are doing. Most administrators will probably turn this setting off after the first couple of reminders.

The leaf objects under sites, domains, or OUs are always going to be links. The only place where you would find yourself looking directly at a GPO is under the Group Policy Objects container.

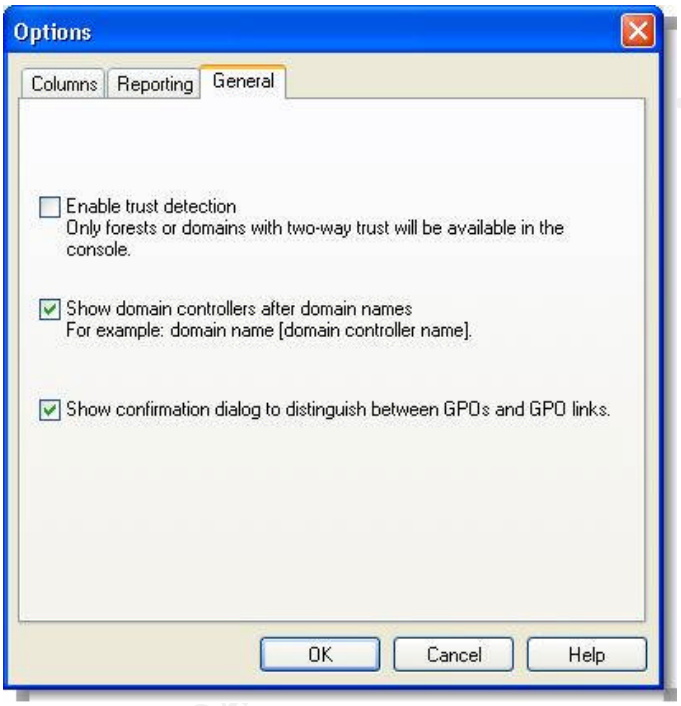

Figure 16: The General tab from the User Interface Options. Allows enabling or disabling of trust detection, showing domain controller names are each domain displayed, and enabling or disabling a confirmation box regarding GPOs vs. GPO links.

ii. Adding Forests and Domains to the Group Policy Management Console Interface

The forest is the highest Active Directory object that is displayed in the GPMC. Sites and domains all fall under these nodes. If you want to manage domains in other forests, you must be able to add the forest itself to the GPMC interface.

In the following example, the two forests to be managed do not trust one another. Both Windows XP and Windows 2003 support a control panel applet called Stored Usernames and Passwords. With it, you can configure credentials for cases such as this one in which you need to access a remote resource but the account which are normally logged on with does not have the necessary rights.

1. Launch the **Stored Usernames and Passwords** from the Control Panel. When the window appears, click on the **"Add"** button.
2. Enter the name of the server or domain that you wish to provide credentials for. Note in the figure below, the server suffix is preceded with an asterisk acting as a wildcard. The reason this was prudent is you can now manage any server with the DNS suffix of SUBSIDIARY.BIZ. Click **"OK"** to return to the original window.

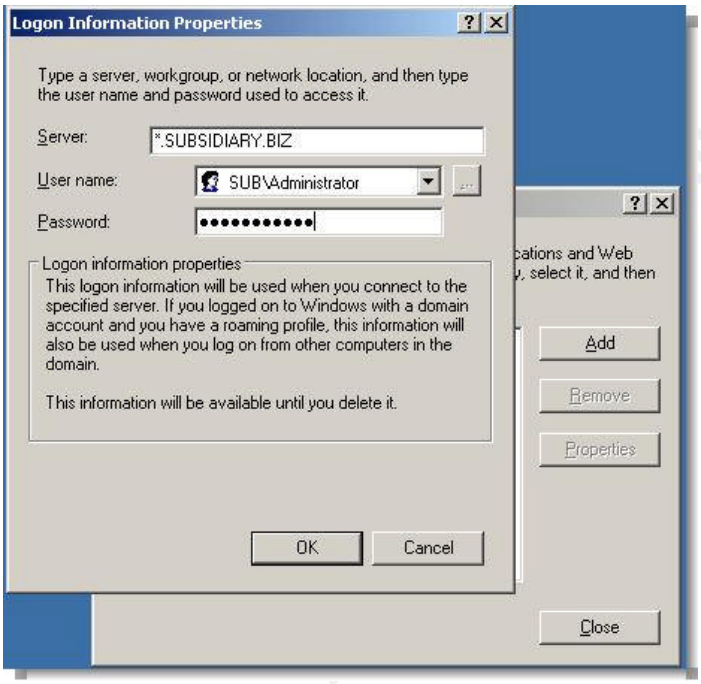

Figure 17: The Stored Usernames and Passwords window that allows you to enter the server name to be accessed and the credentials to use towards that end.

3. The name of the server will now appear in the window that originally opened. In this example, *.SUBSIDIARY.BIZ.
4. Click the **"Close"** button.
5. Ensure that the **"Enable trust detection"** option is disabled as described in the User Interface Options section.
6. Right click the top node in the GPMC console labeled **"Group Policy Management"**. Select **"Add Forest"** from the menu that appears.
7. Enter the DNS domain name of the root domain (which also corresponds to the forest). If this process seems to hang, it is important to remember that DNS must be able to resolve this name. If using Windows 2003 based DNS servers, you can use conditional forwarding to forward requests for the untrusted domain to the appropriate DNS server for name resolution.

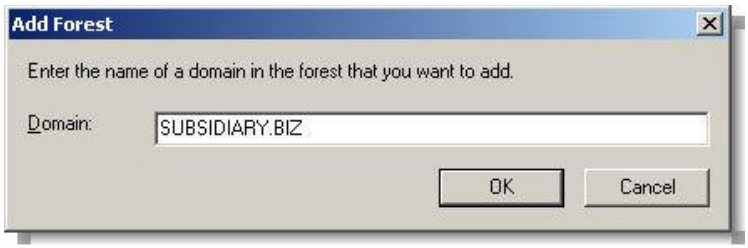

Figure 18: Dialog box allowing you to enter a new domain to be added to the GPMC.

8. Momentarily, the domain will appear in the tree nodes on the left hand side of the GPMC. In the figure below, forest SUBSIDIARY.BIZ has been added. This is a Windows 2000 forest. Note the fact that there is no Group Policy Modeling node in the Windows 2000 domain as this is only supported in a Windows 2003 schema domain with at least one Windows 2003 domain controller.

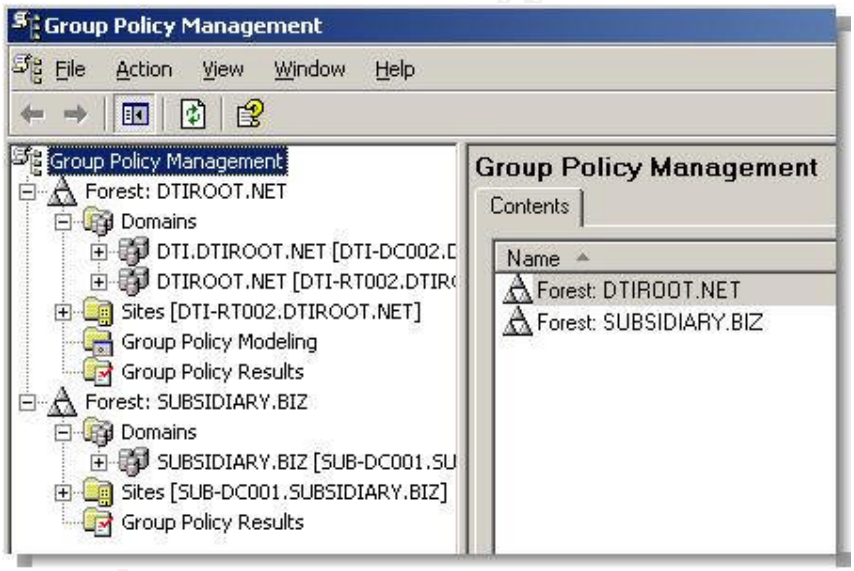

Figure 19: The domain SUBSIDIARY.BIZ has been added to the GPMC. It is not trusted by the DTIROOT.NET domain at all but is manageable due to the credentials entered into the Stored Usernames and Passwords control panel.

9. After the first installation, the GPMC only displays the forest and the domain which contains the administrative account logged in. You can change this as we have seen on the forest level. If you want to add to a domain to the display you must right click the **"Domains"** node within the appropriate forest and select **"Show Domains"** from the menu which appears.
10. The Show Domains window in Figure 20 will appear. Simply check off the domains you want to appear in the interface and click the **"OK"** button.

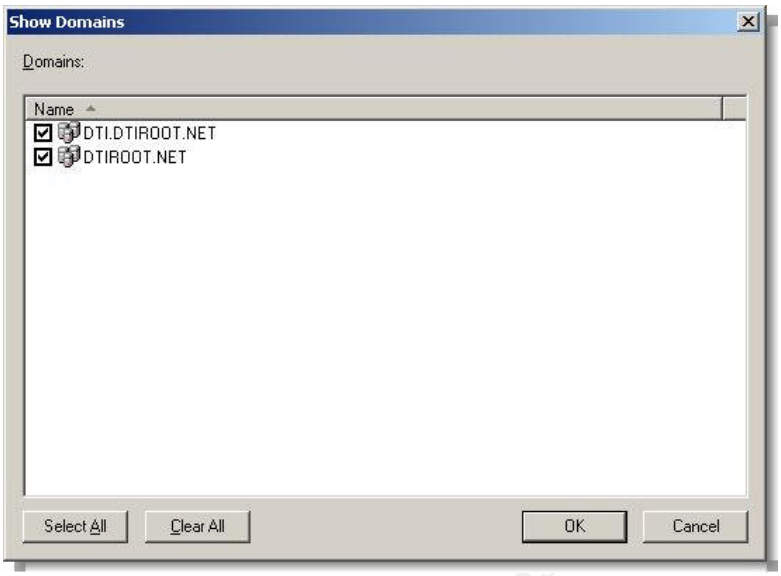

Figure 20: The Show Domains window which allows you to add any of the domains from a particular forest to the GPMC interface.

III. Managing Common Tasks with the Group Policy Management Console

In Chapter 2, an overview of how to perform common tasks with the Windows 2000 Group Policy tools was given. Now we will examine how to perform those same tasks using the GPMC.

i. Creating, Adding, or Deleting Group Policy Objects

Creating and linking a GPO to a site, domain, or OU is quite easy to do using the GPMC. This particular task was not that difficult using the traditional Windows 2000 tools, but there is simply more information that is available at a glance when using the new tool.

- Once the site, domain, or OU is highlighted, you can see any other GPOs linked to it (you could also using the traditional tools) and their precedence. In addition to this, as Figure 21 shows, there is other information that is available in a tabular format that makes it easier to see at a glance a number of properties such as whether or not the link is enforced (referred to as No Override previously), if the link or GPO itself is enabled, etc. Like most other Microsoft tools that display information in this format, the order can be sorted by any of the available columns simply by clicking in the column heading. The order of the columns can be changed by dragging them to the desired position.

- Note the display also shows the Link Order. A Link Order of 1 has the highest precedence. In the event of a conflict in settings between the DTI Executive GP and the DTI Users GP, the DTI Executive GP will be the "winning GPO".
- GPO status is shown. Since these GPOs only have user settings in them, the Computer configuration portion has been disabled to enhance performance.

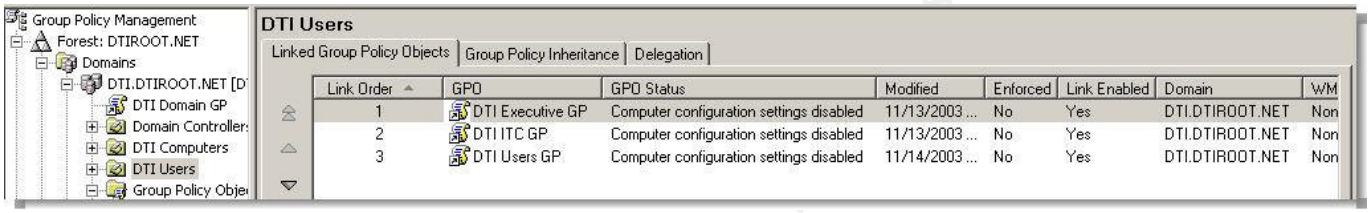

Figure 21: The Linked Group Policy Objects display on an OU. Information is available at a glance in a tabular format that can be ordered by any of the columns in ascending or descending order. The link order of 1 has the highest precedence.

- The Group Policy Inheritance tab shows not only GPOs linked directly to the OU, but those inherited from other OUs. The Precedence column shows which GPOs settings will win in the event of a conflict. A precedence of 1 is, of course, highest.

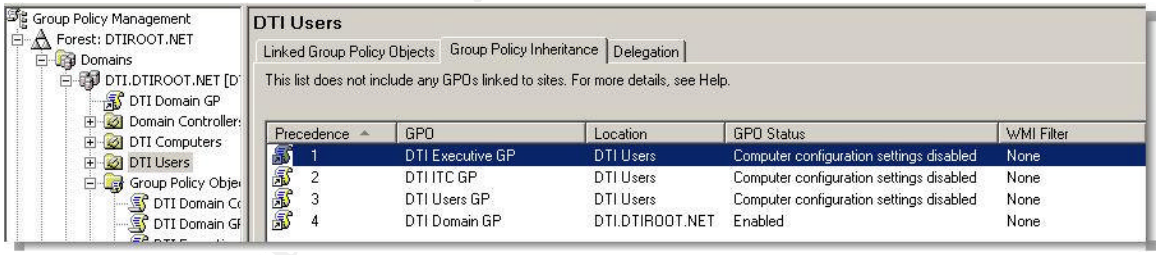

Figure 22: Items displayed on an OUs Group Policy Inheritance tab. This includes the Precedence column.

- The Delegation tab shows which groups or user accounts have the rights to link GPOs to the OU, perform group policy modeling on accounts in the OU, or to read the Group Policy results data. The policy modeling and results data will be discussed in more detail later in this paper.

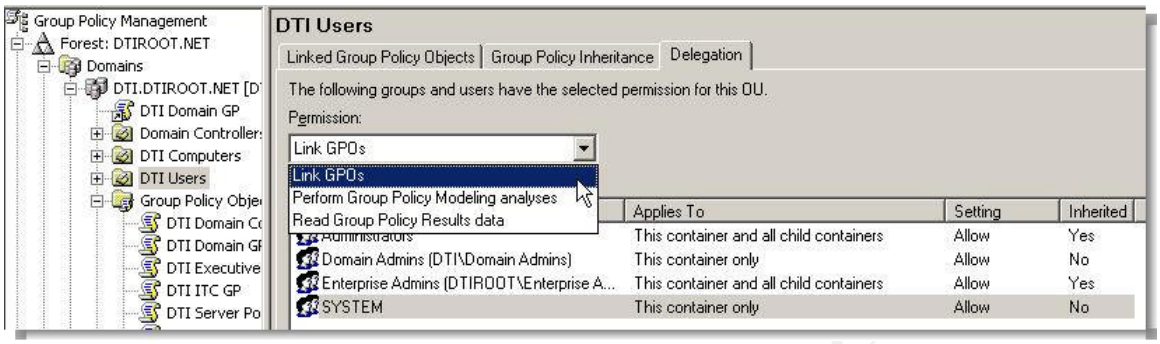

Figure 23: The Delegation tab of an OU. From here you can delegate the right to be able to link GPOs to the OU, run GP modeling analyses (simulation), or read group policy results (actual).

To create a new GPO and immediately link it to a domain, or OU, follow the steps below. Note that on a site object, there is only an option to link a GPO because GPOs are created and stored on a domain basis although they may be linked to other domains or sites later.

1. Right click the domain or OU object and select **"Create and Link a New GPO Here"** from the menu.
2. In the New GPO dialog box, enter the name you want to assign to the GPO and click **"OK".** If you look on the Linked Group Policy Objects tab for the OU, you can see it. In the example below, the Test GPO object was created and given the lowest link order by default. You can change its order by highlighting it and using the arrows along the left hand side of the results pane.

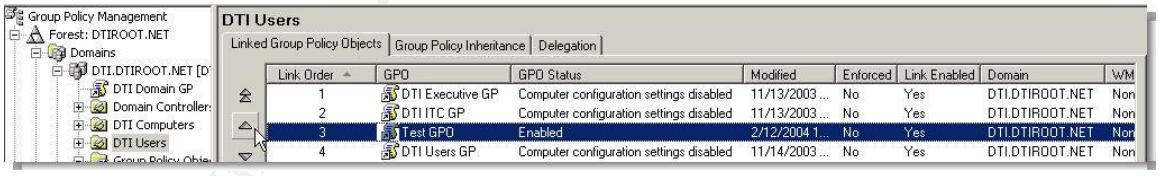

Figure 24: Changing the link order of a newly created GPO linked to the DTI Users OU.

To link an already existing GPO to a site, domain or OU, the process is essentially the same as above only when you right click the object you want to link the GPO to, select **"Link an Existing GPO"** from the menu.

To create a GPO without linking it to an AD object immediately, simply right click the Group Policy Objects container within a domain and select **"New"** from the menu. Enter the name of the GPO and click **"OK"** as before. The GPO will only appear under this container as it has not been linked yet. You can then use the process described above for linking to a site, domain, or OU.

Deleting GPOs and their links is equally straightforward. To delete a link, right click it in the interface and select **"Delete"**. Answer **"OK"** to the confirmation dialog box that warns you it is just a link.

To delete the GPO itself, this must be done by right clicking the GPO under the Group Policy Objects container within a domain and selecting **"Delete"**. This time, answer **"OK"** to the dialog box indicating that the GPO and all links in the domain will be deleted. It is important to note that best practices indicate that you should generally disable a GPO and allows that change to replicate to ensure that all computers governed by that GPO properly remove the settings they received from it before it is removed completely.

ii. Properties of Group Policy Object Links

Clicking on a GPO link reveals the same information in the results pane (the right hand pane of the MMC) as clicking on the actual GPO itself.

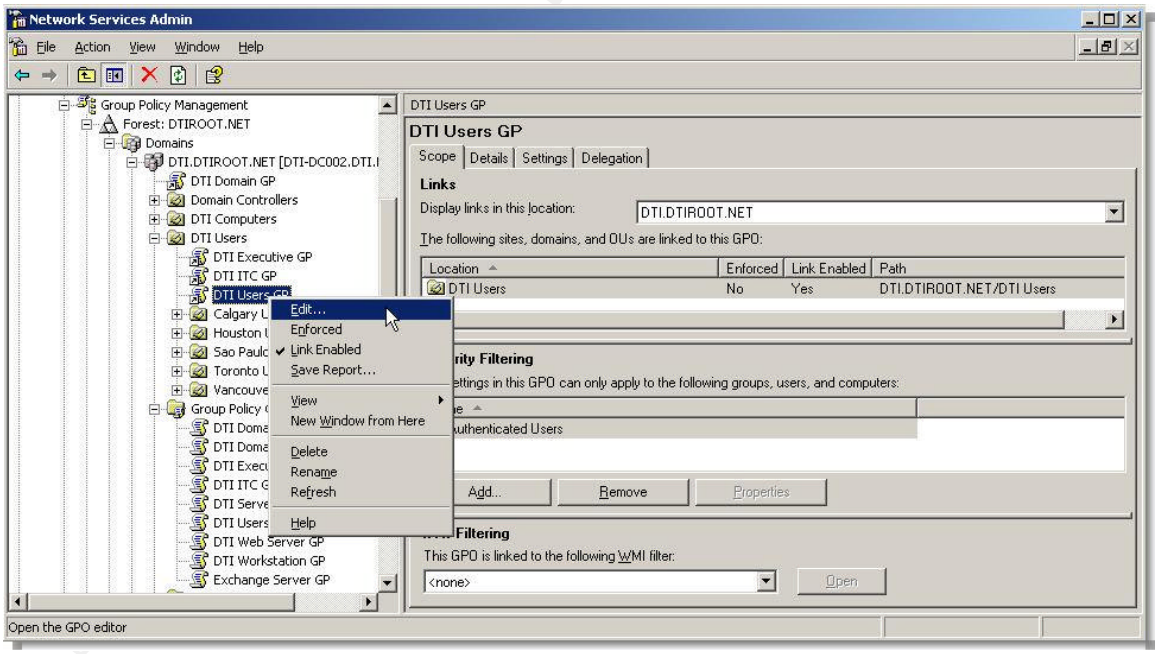

Figure 25: The results pane and menu from a GPO link highlighted in the tree view of the GPMC.

The menu that is revealed is different than clicking on the GPO itself. The options revealed are, for the most part, relevant to a GPO link. Right clicking a GPO has options relevant to it.[6]

[6] Lundy, Jim. "Administering Group Policy with Group Policy Management Console". Group Policy Results. April, 2003. URL: http://download.microsoft.com/download/a/9/c/a9c0f2b8-4803-4d63-8c32-3040d76aa98d/GPMC_Administering.doc (February 5th, 2004)

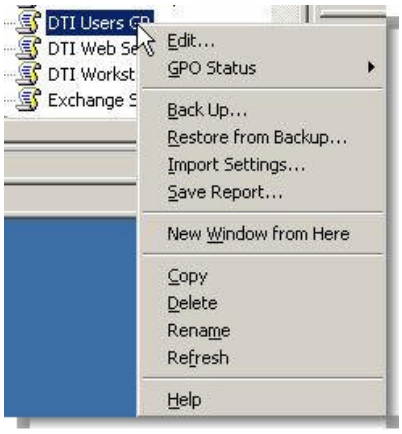

Figure 26: The menu revealed when right clicking an actual GPO object. Compare to the menu displayed in Figure 25.

The following is a discussion of the various tabs available in the results pane for a GPO link and a GPO.

1. **The GPO Link Context Menu:** The options of interest on this menu are:
    a. **Edit:** Clicking this option will launch the GPO Editor for editing the GPO.
    b. **Enforced:** This is the option previously known as No Override using the Windows 2000 GPO tools. When this is set, even if an administrator for a lower level OU sets his to block policy inheritance, the settings from an enforced link will still take effect.
    c. **Save Report:** Clicking this will save an HTML report of all the settings within the GPO to a location you specify.
2. **The Scope Tab:** This tab, pictured in Figure 25, displays all of the places that the GPO is linked to with the following options:
    a. The Active Directory forest in which it resides.
    b. All of the AD sites within the forest.
    c. Domains within the forest.

    You can select these options using the drop down list box on that tab as pictured below.

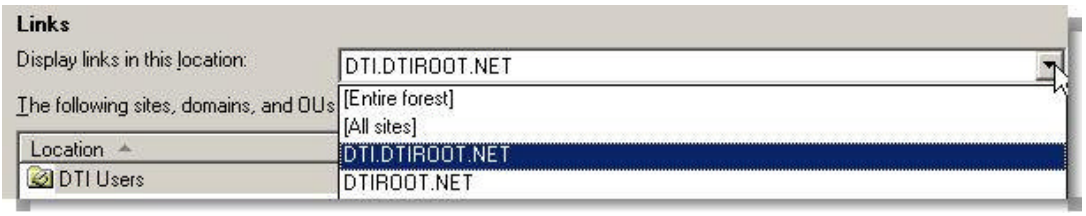

Figure 27: The options available for displaying GPO links on Scope tab for a GPO or GPO link.

The Location section of the tab shows the actual object to which the GPO is linked, whether the link is enforced (previously referred to as No Override), whether the link is enabled, and the path in AD to the container. By right clicking directly on the object to which the GPO is linked in the Location area, you have the options to enforce the link, delete it, enable it (it should show a check mark by default if it is appearing that section in the first place).

The Security Filtering portion displays the users, computers, and groups that can apply the particular GPO. In other words, it summarizes those groups that have at least Read and Apply Group Policy permissions. You can use the Add or Remove buttons to do as their names imply.

Finally, the WMI filter section shows any WMI filters that are linked to that particular GPO. WMI filters are new to Windows 2003 Group Policy and allow policy administrators to choose to apply policy based on specific properties of a computer that can be queried using WMI query language.

WMI or Windows Management Instrumentation is Microsoft's implementation of WBEM or Web Based Enterprise Management. It is an initiative to develop a non-vendor specific means of defining and sharing management information between computer systems.[7] In order for WMI filters to be used in a domain, the Windows 2003 scheme must be in place and at least one domain controller running Windows 2003.

Essentially, things such as the OS type or certain types of hardware can be queried. If the result is true (as evaluated on the client), then the GPO will be applied.

[7] "Windows Management and Instrumentation: Background and Overview". 1999 URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/evaluate/featfunc/wmiovw.asp (February 3rd, 2004)

3. **The Details Tab:** Is just that. It provides details specific to the GPO itself as displayed in the figure below. Most of the items are self explanatory. The ones that bear further discussion are:
    a. **User and Computer Versions:** Any time changes are made to the user or computer portion respectively of a GPO, the version number is incremented. The important thing to remember is that it doesn't matter if the version numbers between the user and computer portions match. However, if there is a mismatch between the AD and SYSVOL portions, then there is a problem. It means that the AD is out of synch with the portion of Group Policy stored in the file system and clients will receive incorrect settings.
    b. **GPO Status:** Shows the current state of the GPO. It is the only configurable item on the Details tab. Using the drop down list box, you can set the status to one of the four options in Figure 28.

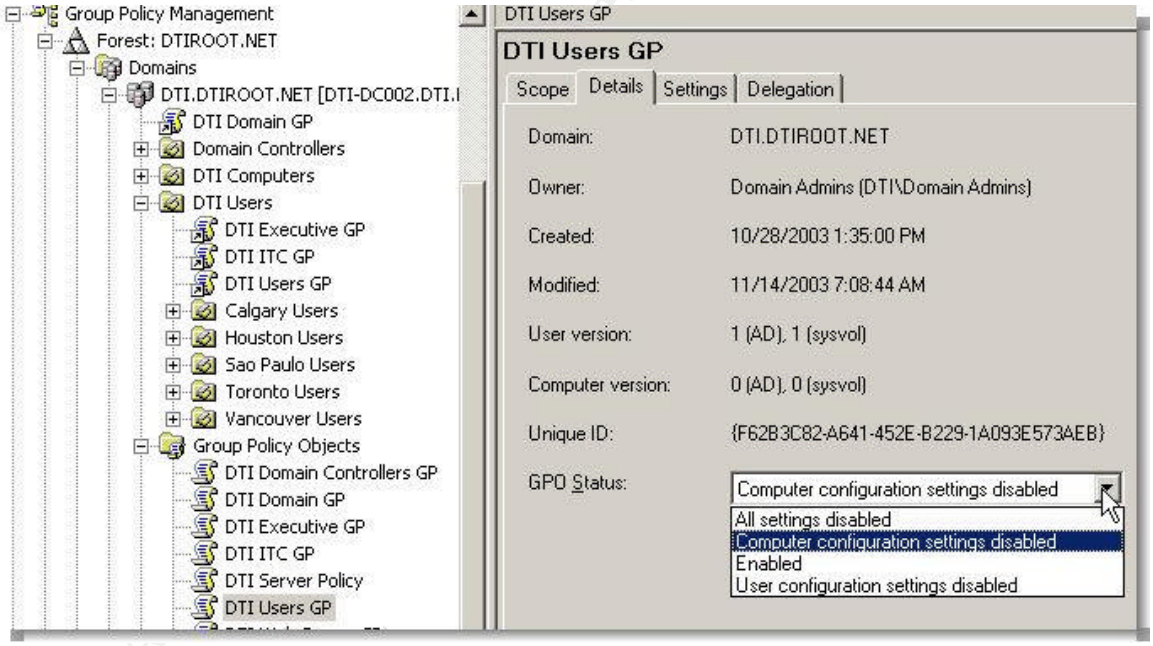

Figure 28: The Details tab of the results pane for a GPO/GPO Link. The only configurable item is to disable a portion of the GPO (user, computer, or both).

4. **The Delegation Tab:** This tab shows all the user, computers, and groups that have permissions on the GPO and what those permissions are in a simplified view. The simplified permissions correspond to those that would be found by using the ACL editor which was the only way to set these permissions in the past. For more granular control, the ACL editor is available by clicking on the **"Advanced"** button on the Delegation tab. The permissions

in the ACL and the corresponding permissions from the GPMC are shown in the table below for comparison.

GPO Delegation Permission in GPMC	Corresponding Permissions from ACL Editor	Comments
Read (from Security Filtering)	Read and Apply Group Policy	Members of a group with these permissions will apply the settings from the GPO.
Edit Settings	Read, Create All Child Objects, Delete All Child Objects, Special Permissions. Implicit deny of Apply Group Policy	Can edit all settings but cannot modify the security on the object. Will not apply the policy.
Edit settings, delete, modify security	Essentially Full Control on the object but without applying the policy.	Can edit everything and set security but will not apply policy.

Table 2: Permissions for the GPO as they appear on the Delegation tab of a GPO and the corresponding ACLs from the ACL Editor. The ACL Editor can be used for more granular control by clicking on the Advanced button.

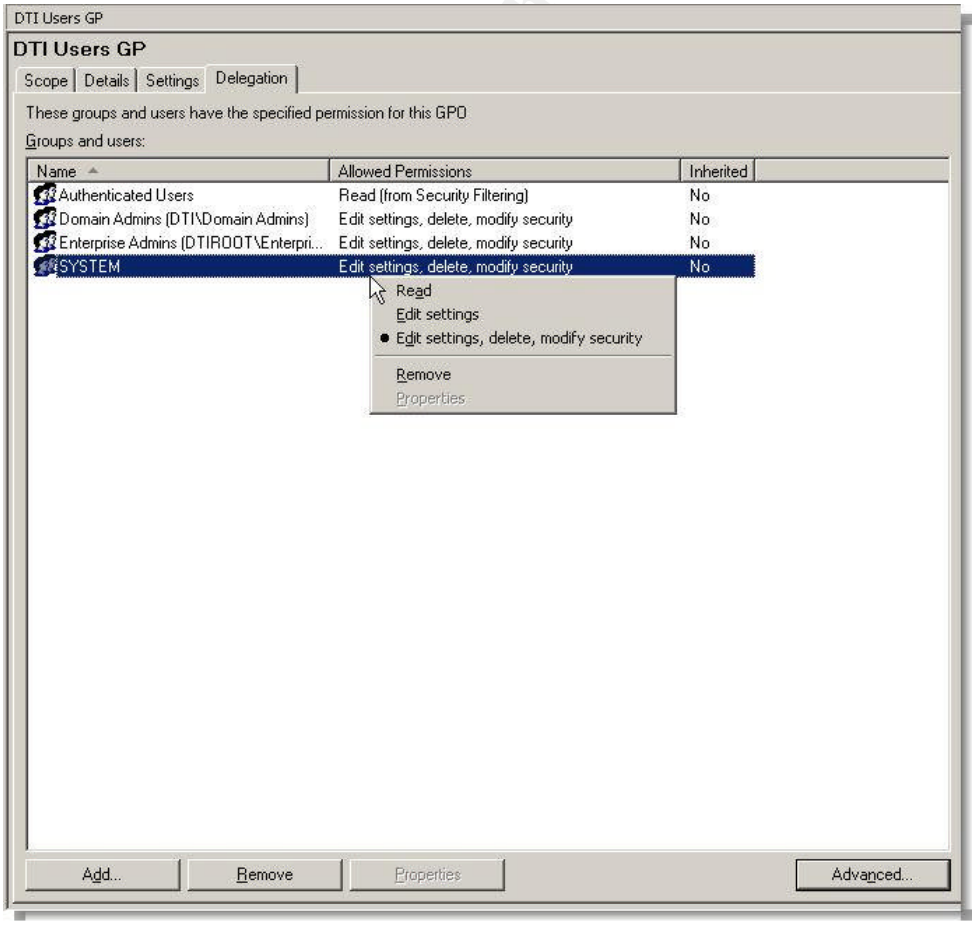

Figure 29: The Delegation tab of a GPO/GPO Link. Displays permissions

5. **The Settings Tab:** The settings tab as stated earlier, is one of the most useful displays of information in the entire GPMC. It provides an HTML report of all the configured settings within a GPO. Each of the individual sections can be expanded or contracted to reveal the settings underneath.

   Right clicking the report will allow you to save it (in HTML or XML format), print it, or launch the GPO Editor to change the settings if need be. The reporting function is especially useful for a couple of reasons:

   a. As previously mentioned, administrators who needed to be able to see how a GPO was configured, but did not have rights to edit the GPO, could not view these settings even if they did have Read permissions. The reason was that the only vehicle for looking at the settings was the GPO Editor which checked for the Edit permission and wouldn't allow access otherwise.
   b. Some settings have, what could be termed anomalous behavior in comparison to the way they behave when being viewed or edited. The most obvious example is trying to work with the Internet Explorer Maintenance settings. More specifically, the Security Zones and Content Ratings. When modifying these settings or even simply viewing them using the GPO Editor, they import the corresponding settings from the machine being used. So administrators would have to be cautious that they did not open this node from a machine that could introduce incorrect settings. The reporting doesn't help the situation if there is a need to edit the IE Maintenance Security portion of the GPO, but does if all that is needed is to read the settings for informational purposes.

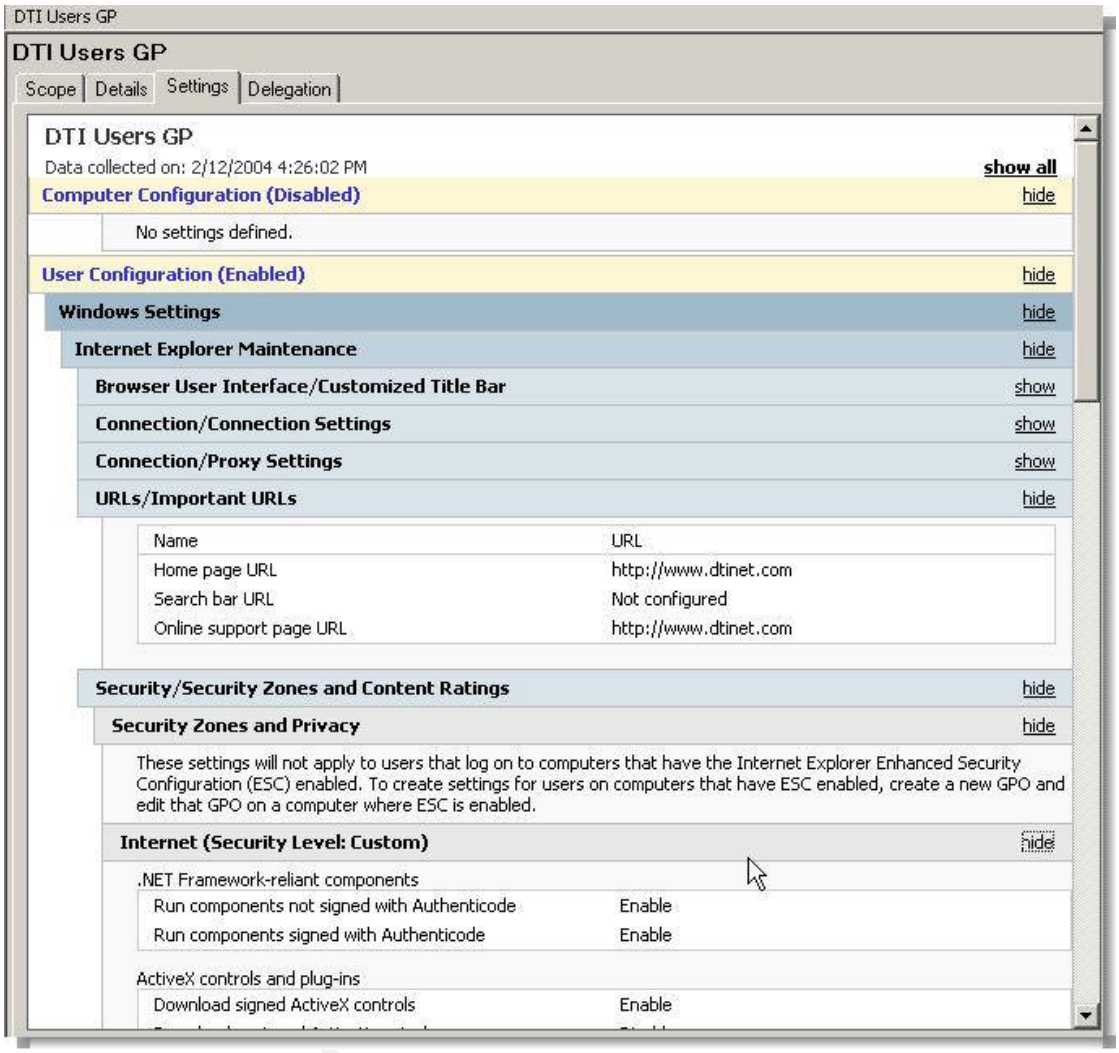

Figure 30: The Settings tab of a GPO. Displays an HTML report of the settings within the GPO. All that is needed is Read permissions. This capability is especially useful in the case of Internet Explorer Maintenance settings which would normally import the settings from the workstation being used to edit the GPO using the Editor.

iii. Properties of Group Policy Objects

The results pane of a GPO is identical to what is displayed when highlighting a GPO link. That said, when right clicking the GPO itself under the Group Policy Objects container, there are some menu options unique to it. They are:

1. **GPO Status:** This provides the same options that would be displayed on the Details tab (described in the previous section). Allows you to enable or disable the entire GPO or the user or computer portions.
2. **Back Up:** This is one of the new features that were not previously available with any of the standard tools from Microsoft.

You can back up one or more GPOs to the file system so, in the event that something ever goes wrong with production GPOs, they can be restored. In fact, using this feature facilitates moving GPOs between domains, or even forests.

To back up a single GPO, simply right click and choose **"Back Up"** from the menu. The Back up Group Policy Object windows appears as depicted in the figure below. Simply enter the path you wish to save the GPO to and click on the Back Up button.

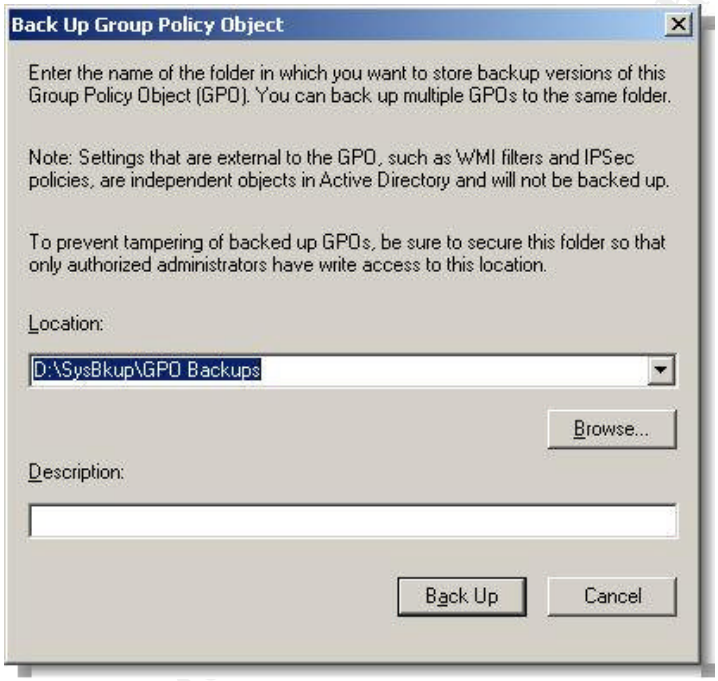

Figure 31: The Back up Group Policy Object window. Enter the file location to back up the GPO(s) to and click Back Up.

To back up all GPO objects at once, right click the Group Policy Objects container in the GPMC and select **"Back Up All"**. You will be presented with the same window as seen in Figure 31. Click the **"Back Up"** button to begin the process.

When finished, the status window will show if everything went OK. Again, this is the same window that would be displayed for a single GPO back up or multiple back ups. Figure 32 shows an example.

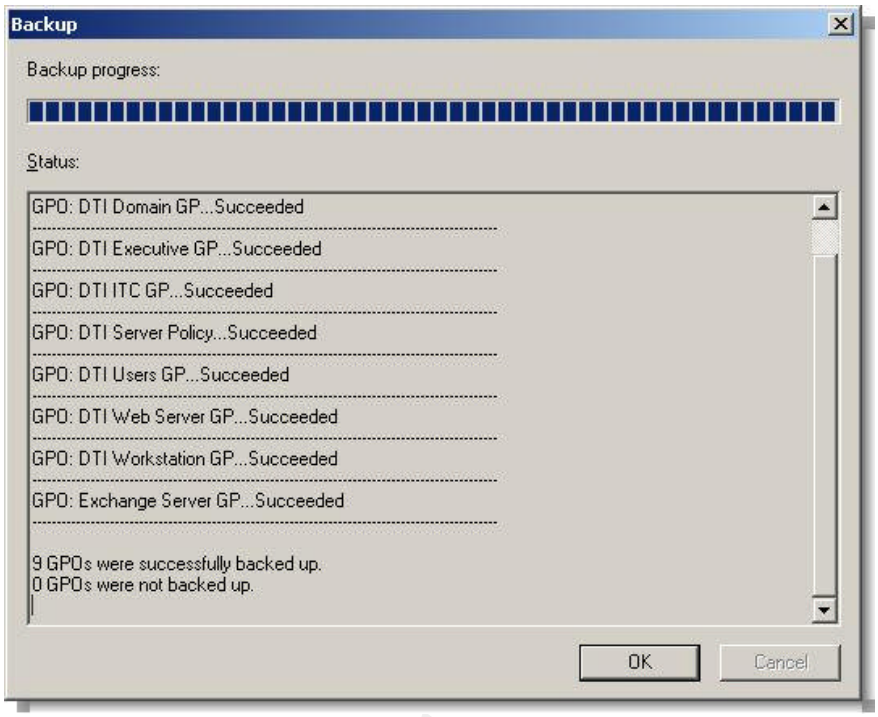

Figure 32: The Backup window shows the progress of the process until complete. It will show the status of each of the individual backups if multiple GPOs were selected.

3. **Restore from Back Up:** A restoration of a GPO can recover a GPO even if it has been deleted completely from the domain. A restore not only recovers the settings, but other information such as the permissions on the GPO, any WMI filter links (but not the filters themselves, and the GPO GUID.[8] Since we are discussing the option as a context menu item on the object itself, for the purposes of this example, we will assume that a number of settings within the GPO were lost somehow.

    a. That being the case, one could simply right click the GPO and select the **"Restore from Back Up"** option that appears. The Group Policy Object Restore Wizard will appear. Click **"Next"**.
    b. Select the back up location containing the backed up GPO. Then click **"Next"**.
    c. The Source GPO window will appear. Select the GPO with the correct name and timestamp (multiple versions can be backed up). You can use the **"View"** button to see

[8] Lundy, Jim. "Administering Group Policy with Group Policy Management Console". Group Policy Results. April, 2003
URL: http://download.microsoft.com/download/a/9/c/a9c0f2b8-4803-4d63-8c32-3040d76aa98d/GPMC_Administering.doc (February 11th, 2004)

the settings within the GPO to confirm that it is truly one that should be restored. When ready, click **"Next"**.

d. Review the information in the Summary window and then click Finish. Another window similar to the progress window depicted in Figure 32 will appear. It will show if the restore succeeded or not.
e. The GPO will be visible once again under the Group Policy Objects container in the GPMC.

4. **Import Settings:** Unlike the restoration process, the only thing that importing does is to completely replace the settings within an existing GPO and replace them with those from the backed up GPO. It does not change ACLs, links, etc. This tool is one method of moving GPOs across domains, even ones with no trust relationships between them.

   In the following example, the settings from a GPO in the Windows 2003 based DTI.DTIROOT.NET domain were imported into the untrusted Windows 2000 domain SUBSIDIARY.BIZ. Recall in the configuration portion of this chapter we set up SUBSIDIARY.BIZ to be managed from our GPMC.

   a. Expanded the SUBSIDIARY.BIZ forest and navigated to the Group Policy Objects container.
   b. Right clicked the SUB Users GP GPO and selected **"Import Settings"**. When the Import Settings Wizard appears, **"Next"** was clicked.
   c. The option to back up the existing GPO (to be imported into) was given. This is a good option to take should anything ever go wrong with the import process or if the settings within the imported GPO cause unexpected issues. The same process to back up GPOs was followed after clicking the **"Backup"** button. Then clicked **"Next"**.
   d. The next screen allowed the location of the restoration files to be chosen. Clicked **"Next"**.
   e. The DTI Users GP object was selected. The check box to only show the most recent version was checked off in case there were older backups copied to the same file system location. Clicked **"Next"**.

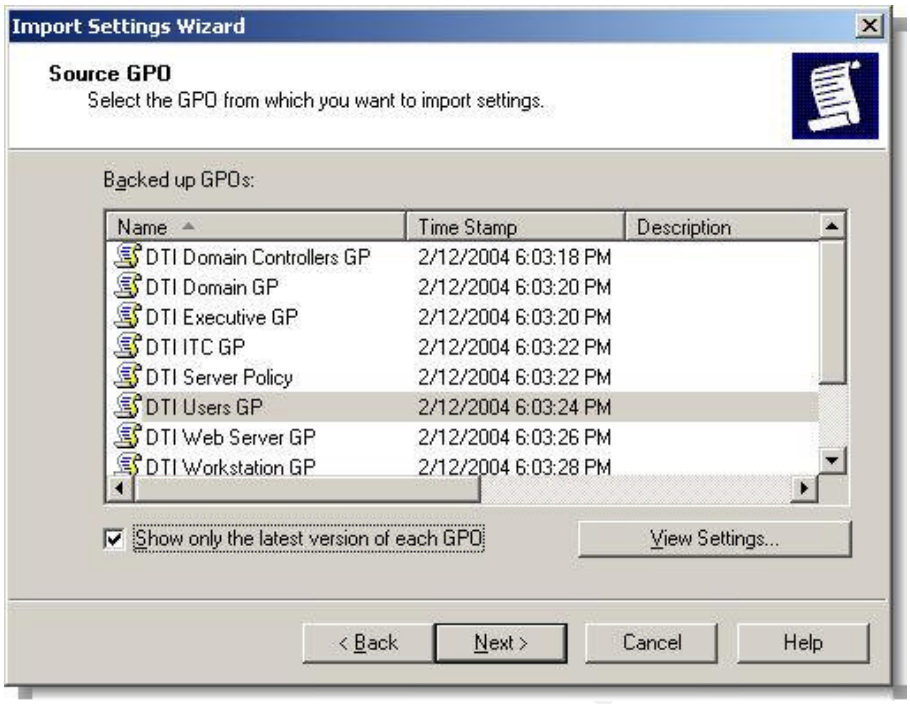

Figure 33: Screen from the Import Settings Wizard allowing the backed up GPO to be selected for the import process. DTI Users GP was chosen. Note the "Show only the latest version of each GPO" option was selected.

f. The next screen scans the settings to determine if any security principals need to be migrated. If this were the case, then Migration Tables would have had to been used. These would allow for a security principal (such as a group) that didn't exist in the importing domain to be mapped to one there. In this instance, there were no security principals to be migrated. Once the scan was complete, **"Next"** was clicked.

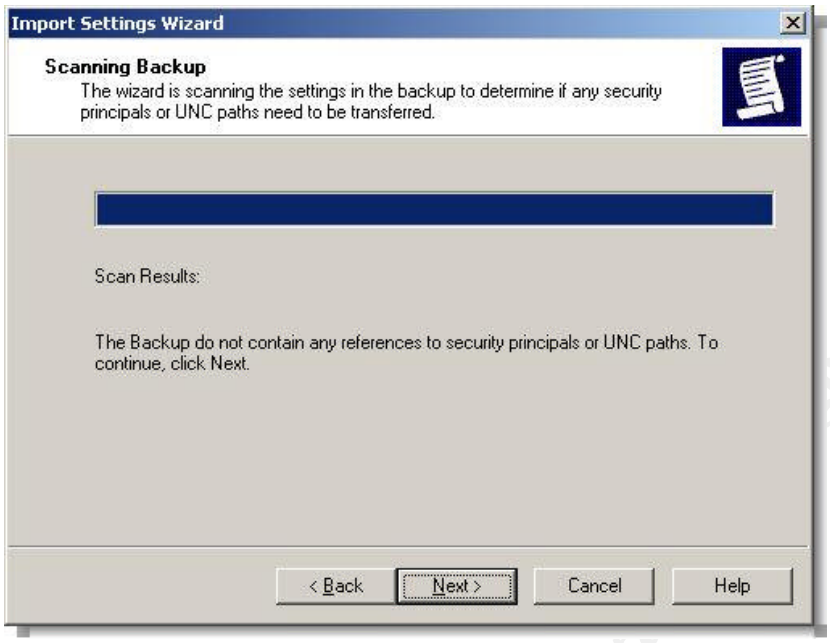

Figure 34: The Scanning Backup screen in the Import Settings Wizard. It determines if there are any security principals that would need to be migrated between the two domains. If that were the case, Migration Tables would have to be used. In this case, it was not necessary.

g. Reviewed the information in the Summary windows and then clicked the **"Finish"** button.
h. A progress window similar to the others used in the back up process appeared and indicated the import completed successfully. Clicked **"OK"** to close the status window.

Using the reporting function, you can examine an imported GPO's settings to determine if the settings you wanted specifically are there in the destination GPO.

Chapter 4: Group Policy Results and Modeling

One of the most significant improvements made since the introduction of Windows XP and now Windows Server 2003 are services that help determine the actual resultant set of policy applied to a machine and another service that allows RSoP data to be planned or modeled before actual implementation, even in a lab.

I. Group Policy Results

RSoP – Logging Mode in Windows XP, now referred to as Group Policy Results in the GPMC, is a tool that allows an administrator to determine the actual set of policies that have been applied to a computer and a user if need be.

Group Policy Results is accessed in the GPMC by right clicking the Group Policy Results node in a domain and starting the **"Group Policy Results Wizard"**. When the wizard opens, click the **"Next"** button.

1. On the Computer Results screen (see Figure), you have the option to display settings for the computer on which it is being run, or another computer. If another computer is selected, that computer must be running Windows XP or Windows 2003.

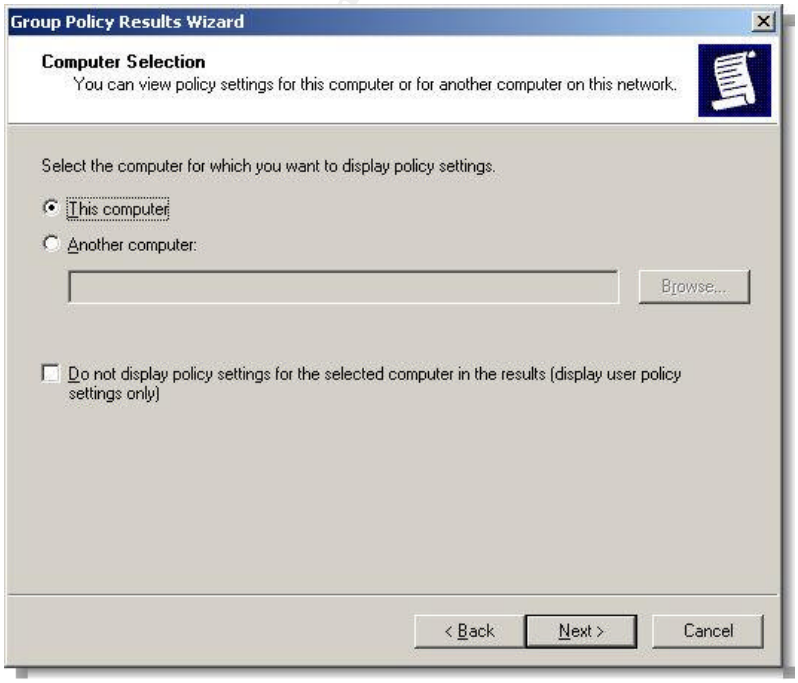

Figure 35: The Group Policy Results Wizard Computer Selection screen.

Also, there is an option to not display the settings for the selected computer, only the user. This is off by default. For the purposes of this example, the defaults were taken and the **"Next"** clicked.

2. On the User Selection screen, your options are to display settings for the logged in user (the default) or another. In the figure below, the user NChristopher was selected from the child domain DTI.DTIROOT.NET.

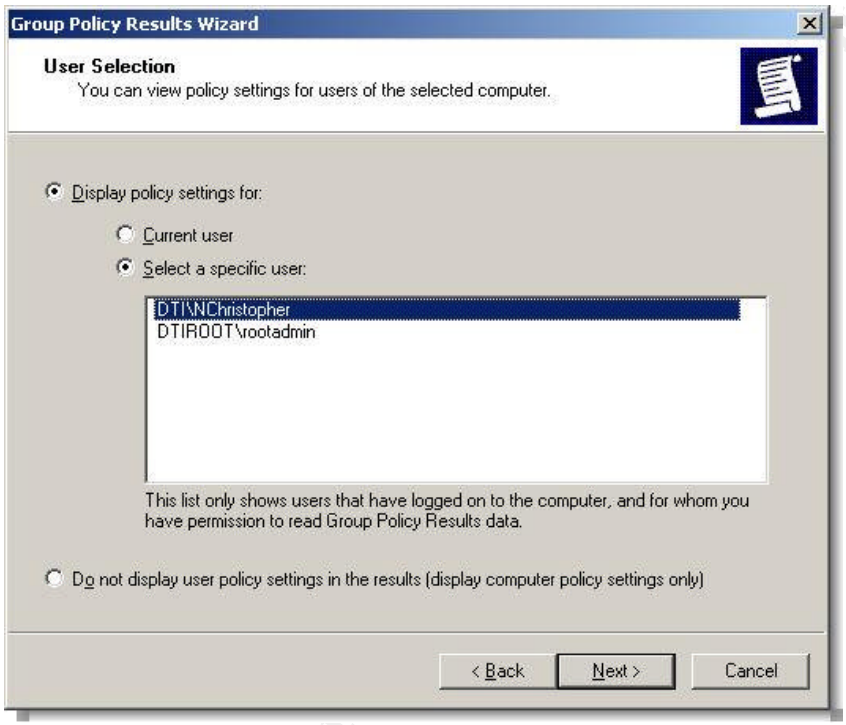

Figure 36: The Group Policy Results Wizard User Selection screen.

3. In the Summary of Selections screen, the selections were examined and then **"Next"** clicked to begin the process. The **"Finish"** button was clicked once it was complete.

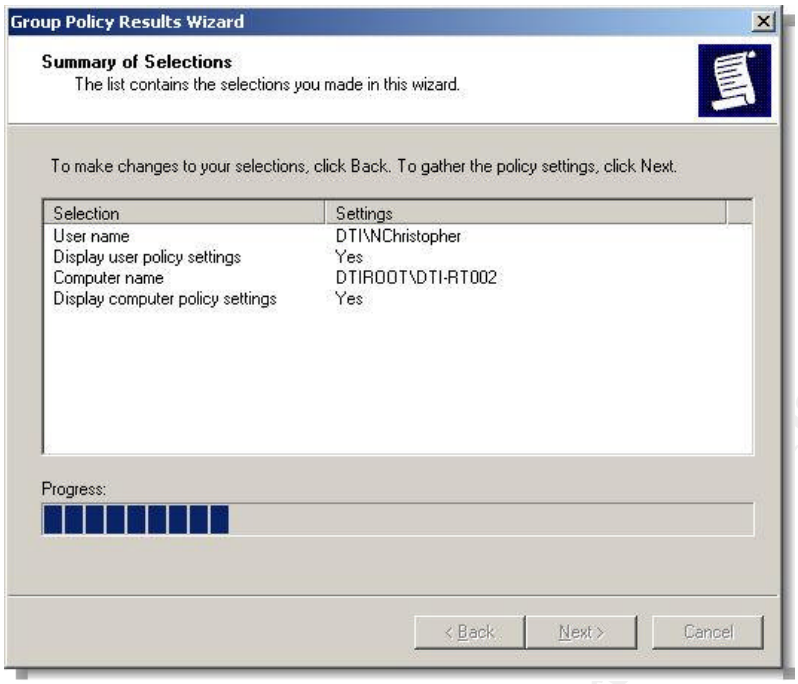

Figure 37: The Group Policy Results Wizard Summary of Selections screen.

Once complete, the results node for NChristopher on DTI-RT002 appears under the Group Policy Results node.

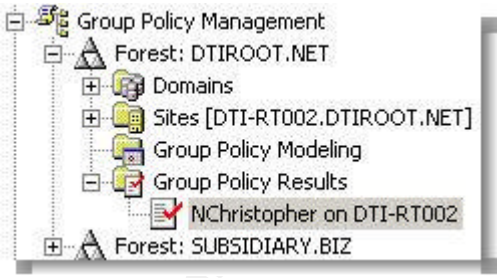

Figure 38: Node for the Group Policy Results for NChristopher on DTI-RT002

Highlighting the node displays the following tabs in the right hand GPMC results pane.

- **Summary:** This displays a large amount of summary data about the policies that were applied. Examples include Applied and Denied GPOs for user and computer configurations, security group membership summaries, component status, etc. See the appendix for an example.
- **Settings:** This tab will show all of the settings that were applied to both the user and computer. It looks very similar to the reports generated for GPOs only there is another column indicating the winning GPO. The GPO from which the setting came.

- **Policy Events:** Simply shows an amalgam of policy related events from the Application Event Log. This is a great tool for troubleshooting problems as all other non-policy events are filtered out.

II. Group Policy Modeling

Group Policy Modeling allows for the simulation of RSoP data (known as RSoP – Planning Mode in Windows XP). A Windows Server 2003 service provides this functionality and therefore explains the requirement for the Windows 2003 schema and at least one Windows 2003 domain controller for the node to even appear in the GPMC.

For the most part, the output for Group Policy Modeling will be similar to the output for the Results. The only two differences are that the results are simulated and there is a query tab instead of the Policy Events tab. The Query tab displays the parameters used to generate the results.

The wizard is started by right clicking the Group Policy Modeling node. Then a number of parameters are selected throughout the process. The figure below summarizes the parameters used and the information that is shown on the Query tab.

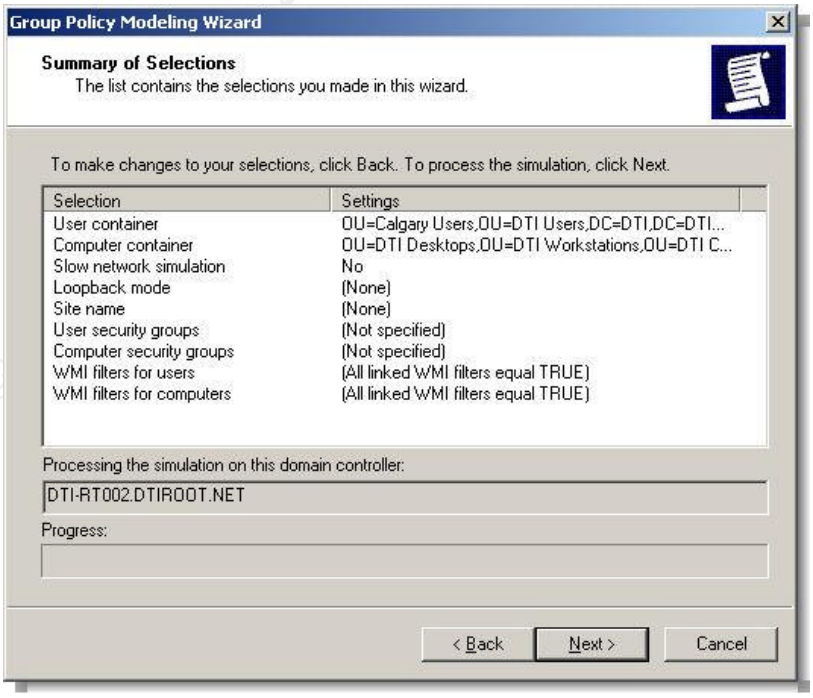

Figure 39: Summary of the parameters used for the Group Policy Modeling Wizard.

Conclusion

The Group Policy Management Console introduces a level of manageability to Windows Group Policy that should have been there from the very beginning. Now businesses should not be forced into seeking potentially expensive third party tools in order to be able to properly manage Group Policy in their environment.

Although not perfect, the GPMC introduces enough useful functionality to make it a must have for administrators and security administrators alike.

Appendix

Group Policy Results

DTI\nchristopher on DTIROOT\DTI-RT002

Data collected on: 2/12/2004 8:43:25 PM **hide all**

Summaryhide

Computer Configuration Summaryhide

Generalhide

Computer name	DTIROOT\DTI-RT002
Domain	DTIROOT.NET
Site	Calgary
Last time Group Policy was processed	2/12/2004 8:38:02 PM

Group Policy Objectshide

Applied GPOshide

Name	Link Location	Revision
Local Group Policy	Local	AD (1), Sysvol (1)
DTI Server Policy	DTIROOT.NET/Configuration/Sites/Calgary	AD (5), Sysvol (5)
Root Domain GP	DTIROOT.NET	AD (7), Sysvol (7)
DTI Domain Controllers GP	DTIROOT.NET/Domain Controllers	AD (1), Sysvol (1)

Denied GPOshide

Name	Link Location	Reason Denied

None

Security Group Membership when Group Policy was appliedhide

BUILTIN\Administrators
Everyone
BUILTIN\Pre-Windows 2000 Compatible Access
BUILTIN\Windows Authorization Access Group
NT AUTHORITY\NETWORK
NT AUTHORITY\Authenticated Users
NT AUTHORITY\This Organization
DTIROOT\DTI-RT002$
DTIROOT\Domain Controllers
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS

WMI Filtershide

Name	Value	Reference GPO(s)

None

Component Statushide

Component Name	Status	Last Process Time
Group Policy Infrastructure	Success	2/12/2004 8:38:02 PM
EFS recovery	Success (no data)	11/16/2003 9:43:29 PM
Registry	Success	11/16/2003 9:43:25 PM
Security	Success	2/11/2004 1:50:31 AM

User Configuration Summaryhide

Generalhide

User name	DTI\nchristopher
Domain	DTI.DTIROOT.NET
Last time Group Policy was processed	11/27/2003 9:12:32 PM

Group Policy Objectshide

Applied GPOshide

Name	Link Location	Revision
DTI Domain GP	DTI.DTIROOT.NET	AD (7), Sysvol (7)
DTI Users GP	DTI.DTIROOT.NET/DTI Users	AD (1), Sysvol (1)

Denied GPOshide

Name	Link Location	Reason Denied
Local Group Policy	Local	Empty
DTI ITC GP	DTI.DTIROOT.NET/DTI Users	Empty
DTI Executive GP	DTI.DTIROOT.NET/DTI Users	Empty

Security Group Membership when Group Policy was appliedhide

DTI\Domain Users
Everyone
BUILTIN\Pre-Windows 2000 Compatible Access
BUILTIN\Administrators
NT AUTHORITY\INTERACTIVE
NT AUTHORITY\Authenticated Users
NT AUTHORITY\This Organization
LOCAL
DTI\ITC Sys Admins
DTI\ITC
DTI\ITC Net Support
DTI\Domain Admins
DTI\ITC E-mail Admins
DTIROOT\ITC Data Recovery
DTIROOT\ITC Issuing CA Admins
DTIROOT\Enterprise Admins
DTIROOT\ITC High Sec CA Admins

WMI Filtershide

Name	Value	Reference GPO(s)
None		

Component Statushide

Component Name	Status	Last Process Time
Group Policy Infrastructure	Success	11/27/2003 9:12:32 PM
Internet Explorer Branding	Success	11/27/2003 12:45:26 PM
Registry	Success	11/27/2003 12:45:24 PM

Computer Configurationhide

Windows Settingshide

Security Settingshide

Account Policies/Password Policyhide

Policy	Setting	Winning GPO
Enforce password history	1 passwords remembered	Root Domain GP
Maximum password age	42 days	Root Domain GP
Minimum password age	0 days	Root Domain GP

Minimum password length	0 characters	Root Domain GP
Password must meet complexity requirements	Disabled	Root Domain GP
Store passwords using reversible encryption	Disabled	Root Domain GP

Account Policies/Account Lockout Policy hide

Policy	Setting	Winning GPO
Account lockout threshold	0 invalid logon attempts	Root Domain GP

Account Policies/Kerberos Policy hide

Policy	Setting	Winning GPO
Enforce user logon restrictions	Enabled	Root Domain GP
Maximum lifetime for service ticket	600 minutes	Root Domain GP
Maximum lifetime for user ticket	10 hours	Root Domain GP
Maximum lifetime for user ticket renewal	7 days	Root Domain GP
Maximum tolerance for computer clock synchronization	5 minutes	Root Domain GP

Local Policies/Audit Policy hide

Policy	Setting	Winning GPO
Audit account logon events	No auditing	DTI Domain Controllers GP
Audit directory service access	No auditing	DTI Domain Controllers GP
Audit logon events	No auditing	DTI Domain Controllers GP
Audit object access	No auditing	DTI Domain Controllers GP
Audit policy change	No auditing	DTI Domain Controllers GP
Audit privilege use	No auditing	DTI Domain Controllers GP
Audit process tracking	No auditing	DTI Domain Controllers GP
Audit system events	No auditing	DTI Domain Controllers GP

Local Policies/User Rights Assignment hide

Policy	Setting	Winning GPO
Access this computer from the network	Everyone, Administrators, Authenticated Users	DTI Domain Controllers GP
Act as part of the operating system		DTI Domain Controllers GP
Add workstations to domain	Authenticated Users	DTI Domain Controllers GP
Adjust memory quotas for a process	Administrators	DTI Domain Controllers GP
Allow log on locally	TsInternetUser, Administrators, Backup	DTI Domain Controllers GP

	Operators, Account Operators, Server Operators, Print Operators	
Back up files and directories	Administrators, Backup Operators, Server Operators	DTI Domain Controllers GP
Bypass traverse checking	Everyone, Administrators, Authenticated Users	DTI Domain Controllers GP
Change the system time	Administrators, Server Operators	DTI Domain Controllers GP
Create a pagefile	Administrators	DTI Domain Controllers GP
Create a token object		DTI Domain Controllers GP
Create permanent shared objects		DTI Domain Controllers GP
Debug programs	Administrators	DTI Domain Controllers GP
Deny access to this computer from the network		DTI Domain Controllers GP
Deny log on as a batch job		DTI Domain Controllers GP
Deny log on as a service		DTI Domain Controllers GP
Deny log on locally		DTI Domain Controllers GP
Enable computer and user accounts to be trusted for delegation	Administrators	DTI Domain Controllers GP
Force shutdown from a remote system	Administrators, Server Operators	DTI Domain Controllers GP
Generate security audits		DTI Domain Controllers GP
Increase scheduling priority	Administrators	DTI Domain Controllers GP
Load and unload device drivers	Administrators	DTI Domain Controllers GP
Lock pages in memory		DTI Domain Controllers GP
Log on as a batch job		DTI Domain Controllers GP
Log on as a service		DTI Domain Controllers GP
Manage auditing and security log	Administrators	DTI Domain Controllers GP
Modify firmware environment values	Administrators	DTI Domain Controllers GP
Profile single process	Administrators	DTI Domain Controllers GP
Profile system performance	Administrators	DTI Domain Controllers GP
Remove computer from docking station	Administrators	DTI Domain Controllers GP
Replace a process level token		DTI Domain Controllers GP
Restore files and directories	Administrators, Backup Operators, Server Operators	DTI Domain Controllers GP

Shut down the system	Administrators, Backup Operators, Account Operators, Server Operators, Print Operators	DTI Domain Controllers GP
Synchronize directory service data		DTI Domain Controllers GP
Take ownership of files or other objects	Administrators	DTI Domain Controllers GP

Local Policies/Security Optionshide

Microsoft Network Serverhide

Policy	Setting	Winning GPO
Microsoft network server: Digitally sign communications (if client agrees)	Enabled	DTI Domain Controllers GP

Network Securityhide

Policy	Setting	Winning GPO
Network security: Force logoff when logon hours expire	Disabled	Root Domain GP

Public Key Policies/Autoenrollment Settingshide

Policy	Setting	Winning GPO
Enroll certificates automatically	Enabled	[Default setting]
Renew expired certificates, update pending certificates, and remove revoked certificates	Disabled	
Update certificates that use certificate templates	Disabled	

Public Key Policies/Encrypting File Systemhide

Propertieshide

	Winning GPO	[Default setting]
Policy	Setting	
Allow users to encrypt files using Encrypting File System (EFS)	Enabled	

Certificateshide

Issued To	Issued By	Expiration Date	Intended Purposes	Winning GPO
administrator	administrator	9/27/2006 12:53:48 PM	File Recovery	Root Domain

For additional information about individual settings, launch Group Policy Object Editor.

Public Key Policies/Trusted Root Certification Authoritieshide

Propertieshide

	Winning GPO	[Default setting]
Policy	Setting	
Allow users to select new root certification authorities (CAs) to trust	Enabled	
Client computers can trust the following certificate stores	Third-Party Root Certification Authorities and Enterprise Root Certification Authorities	
To perform certificate-based authentication of users and computers, CAs must meet the following criteria	Registered in Active Directory only	

Administrative Templateshide

Systemhide

Policy	Setting	Winning GPO
Display Shutdown Event Tracker	Disabled	Local Group Policy

User Configurationhide

Windows Settingshide

Security Settingshide

Public Key Policies/Autoenrollment Settingshide

Policy	Setting	Winning GPO
Enroll certificates automatically	Enabled	DTI Domain GP
Renew expired certificates, update pending certificates, and remove revoked certificates	Enabled	
Update certificates that use certificate templates	Enabled	

Internet Explorer Maintenancehide

Browser User Interface/Customized Title Barhide

Title Bar Text	Winning GPO
Bantrel	DTI Users GP

Connection/Proxy Settingshide

Winning GPO	DTI Users GP

Enable proxy settings

Protocol	Server	Port
HTTP	HTTP://CGYPRX1	80
Secure	HTTP://CGYPRX1	80
FTP	HTTP://CGYPRX1	80
Gopher	HTTP://CGYPRX1	80
Socks	HTTP://CGYPRX1	80

Exceptions:	Do not use proxy server for addresses beginning with	
	Do not use proxy server for local (intranet) addresses	Enabled

URLs/Important URLshide

Name	URL	Winning GPO
Home page URL	http://www.dtinet.com	DTI Users GP
Search bar URL	Not configured	N/A
Online support page URL	http://www.dtinet.com	DTI Users GP

Administrative Templateshide

Desktophide

Policy	Setting	Winning GPO
Do not add shares of recently opened documents to My Network Places	Enabled	DTI Domain GP

Start Menu and Taskbarhide

Policy	Setting	Winning GPO
Add Logoff to the Start Menu	Enabled	DTI Domain GP
Turn off personalized menus	Enabled	DTI Domain GP

Extra Registry Settingshide

Display names for some settings cannot be found. You might be able to resolve this issue by updating the .ADM files used by Group Policy Management.

Setting	State	Winning GPO
Software\Policies\TerraNovum\EZ_GPO\MajorVersion	1	DTI Domain GP

Software\Policies\TerraNovum\EZ_GPO\MinorVersion	1	DTI Domain GP
Software\Policies\TerraNovum\EZ_GPO\Options\Log	0	DTI Domain GP
Software\Policies\TerraNovum\EZ_GPO\Options\LogFile	%TEMP%\EZ_GPO_log.txt	DTI Domain GP
Software\Policies\TerraNovum\EZ_GPO\Options\LogLevel	1	DTI Domain GP
Software\Policies\TerraNovum\EZ_GPO\Options\SecurityBypass	1	DTI Domain GP
Software\Policies\TerraNovum\EZ_GPO\SettingsScheme	Simple	DTI Domain GP
Software\Policies\TerraNovum\EZ_GPO\Simple\ACMachHibernateIdleTime	0	DTI Domain GP
Software\Policies\TerraNovum\EZ_GPO\Simple\ACUserMonIdleTime	60	DTI Domain GP
Software\Policies\TerraNovum\EZ_GPO\Simple\ACUserStandByIdleTime	0	DTI Domain GP

References

1. Sheesley, John "Understanding System Policies". Microsoft TechNet. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winntas/tips/techrep/systemp.asp. (February 8, 2004)

2. Minasi, Mark. "Mastering Windows Server 2003". San Francisco: Sybex Inc., 2003. 737

3. Mar-Elia, Darren. "The Definitive Guide to Windows 2000 Group Policy". RealTimePublishers.com. 2001. 62

4. Lundy, Jim. "Administering Group Policy with Group Policy Management Console". Group Policy Results. April, 2003 URL: http://download.microsoft.com/download/a/9/c/a9c0f2b8-4803-4d63-8c32-3040d76aa98d/GPMC_Administering.doc (February 3rd, 2004)

5. Otey, Michael. "Windows 2003: An Out of Band Experience" Windows & .NET Magazine September 2003. http://www.winnetmag.com/Article/ArticleID/39778/39778.html (February 7th, 2004)

6. Lundy, Jim. "Administering Group Policy with Group Policy Management Console". Group Policy Results. April, 2003. URL: http://download.microsoft.com/download/a/9/c/a9c0f2b8-4803-4d63-8c32-3040d76aa98d/GPMC_Administering.doc (February 5th, 2004)

7. "Windows Management and Instrumentation: Background and Overview". 1999 URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/evaluate/featfunc/wmiovw.asp (February 3rd, 2004)

8. Lundy, Jim. "Administering Group Policy with Group Policy Management Console". Group Policy Results. April, 2003 URL: http://download.microsoft.com/download/a/9/c/a9c0f2b8-4803-4d63-8c32-3040d76aa98d/GPMC_Administering.doc (February 11th, 2004)