This guide introduces the concepts that drive GPOs, as well as essential knowledge for implementing them for your organization. Key concepts such as precedence, inheritance, and permissions are covered in-depth. You will also be introduced to controlling software and security for every computer in the enterprise using GPOs.

Contents

Introduction
Group Policy Fundamentals
GPO and Active Directory Design Considerations
Controlling GPO Inheritance
Default GPOs and Their Shortcuts
Group Policy User and Computer Configurations
The Final Word
Implementing Group Policy Objects

by Derek Melber

About the Author: Derek Melber runs and operates http://www.auditingwindows.com, the first dedicated Web site for Windows Auditing and Security. There you will find the only books on Auditing Windows. Derek is a contributing editor for Redmond Magazine, as well as providing columns for some of the most distributed Internal Auditor newsletters and journals on the market. This is his first in a series of three GPO books he’s writing for MCPMag.com. You can reach Derek at derekm@braincore.net.

Published July 2004
Table of Contents

Introduction ........................................................................................................................... 7

Group Policy Fundamentals .................................................................................................. 8

What Is a GPO? .................................................................................................................... 8
What Does a GPO Do? .......................................................................................................... 8
What Can a GPO Do? .......................................................................................................... 9
The GPO v. System Policy ................................................................................................... 11

System Policy .................................................................................................................... 11

Group Policy Objects ......................................................................................................... 12

What’s Unique to a GPO .................................................................................................... 13
Where a GPO Can Reside .................................................................................................. 14

GPO Link ........................................................................................................................... 15

What a GPO Affects ........................................................................................................... 17

Basic GPO Functions ....................................................................................................... 19

Creating a New GPO .......................................................................................................... 20

Linking an Existing GPO .................................................................................................. 22

GPO Precedence ............................................................................................................... 24

LSDOU ............................................................................................................................... 24

GPOs within Site, Domain or OU ....................................................................................... 26

Appending and Conflicting Settings ............................................................................... 27

Resultant Set of Policies .................................................................................................. 30

GPO Application ............................................................................................................... 32
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default GPOs and Their Shortcuts</td>
<td>63</td>
</tr>
<tr>
<td>Default GPOs</td>
<td>63</td>
</tr>
<tr>
<td>Default Domain Policy</td>
<td>63</td>
</tr>
<tr>
<td>Default Domain Controller Policy</td>
<td>65</td>
</tr>
<tr>
<td>Account Policies Break the Rule</td>
<td>67</td>
</tr>
<tr>
<td>Account Policies at the Domain Level</td>
<td>68</td>
</tr>
<tr>
<td>Account Policies at the OU Level</td>
<td>68</td>
</tr>
<tr>
<td>GPO Shortcuts</td>
<td>69</td>
</tr>
<tr>
<td>ADUC</td>
<td>69</td>
</tr>
<tr>
<td>Default &lt;Domain/Domain Controller&gt; Security Policy</td>
<td>70</td>
</tr>
<tr>
<td>Local Security Policy</td>
<td>71</td>
</tr>
<tr>
<td>Microsoft Management Console</td>
<td>74</td>
</tr>
<tr>
<td>Gpedit.msc</td>
<td>76</td>
</tr>
<tr>
<td>Group Policy User and Computer Configurations</td>
<td>77</td>
</tr>
<tr>
<td>Computer Configuration</td>
<td>77</td>
</tr>
<tr>
<td>Software Settings</td>
<td>78</td>
</tr>
<tr>
<td>Windows Settings</td>
<td>79</td>
</tr>
<tr>
<td>Scripts (Startup/Shutdown)</td>
<td>80</td>
</tr>
<tr>
<td>Security Settings</td>
<td>81</td>
</tr>
<tr>
<td>Account Policies</td>
<td>81</td>
</tr>
<tr>
<td>Local Policies</td>
<td>81</td>
</tr>
<tr>
<td>Event Log</td>
<td>83</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Restricted Groups</td>
<td>83</td>
</tr>
<tr>
<td>System Services</td>
<td>85</td>
</tr>
<tr>
<td>Registry</td>
<td>86</td>
</tr>
<tr>
<td>File System</td>
<td>87</td>
</tr>
<tr>
<td>Wireless Network (IEEE 802.11) Policies</td>
<td>87</td>
</tr>
<tr>
<td>Public Key Policies</td>
<td>88</td>
</tr>
<tr>
<td>Software Restriction Policies</td>
<td>88</td>
</tr>
<tr>
<td>IP Security Policies on Active Directory</td>
<td>90</td>
</tr>
<tr>
<td>Administrative Templates</td>
<td>91</td>
</tr>
<tr>
<td>Windows Components</td>
<td>92</td>
</tr>
<tr>
<td>System</td>
<td>93</td>
</tr>
<tr>
<td>Network</td>
<td>95</td>
</tr>
<tr>
<td>Printers</td>
<td>96</td>
</tr>
<tr>
<td>User Configuration</td>
<td>96</td>
</tr>
<tr>
<td>Software Settings</td>
<td>96</td>
</tr>
<tr>
<td>Windows Settings</td>
<td>97</td>
</tr>
<tr>
<td>Remote Installation Services</td>
<td>97</td>
</tr>
<tr>
<td>Scripts (Logon/Logoff)</td>
<td>98</td>
</tr>
<tr>
<td>Security Settings</td>
<td>98</td>
</tr>
<tr>
<td>Public Key Policies</td>
<td>98</td>
</tr>
<tr>
<td>Software Restriction Policies</td>
<td>98</td>
</tr>
<tr>
<td>Folder Redirection</td>
<td>98</td>
</tr>
</tbody>
</table>
Internet Explorer Maintenance ................................................................. 100

Administrative Templates ............................................................................. 101

Windows Components .................................................................................... 101

Start Menu and Taskbar .................................................................................. 102

Desktop ............................................................................................................. 103

Control Panel .................................................................................................... 103

Shared Folders .................................................................................................. 103

Network ............................................................................................................. 104

System .............................................................................................................. 104

The Final Word ................................................................................................. 105
Introduction

As you get started with Group Policy (and Group Policy Objects or GPOs), you’ll soon find out that while there is quite a bit of documentation available on the topic, much of it is hard to read or incorrect, missing key facts, or hit and miss with its information. After spending the past four and a half years working with GPOs and the previous five years to that with Windows NT System Policies, I have developed a methodical approach to thinking about, designing, implementing and troubleshooting GPOs. In this digital report I cover the basics. In the next volume, I’ll crank it up a notch and address more advanced topics. In the third volume, I’ll provide insights about how to troubleshoot Group Policies. I’m glad you’re coming along for the ride!

There is no debate that GPOs are a vital aspect of any Windows Active Directory enterprise and network. This digital report discusses the essential aspects of GPOs to give you understanding and confidence to implement them in your Active Directory environment. The book has four sections. First, you need to get a good solid foundation of GPOs, which will be covered in the opening section, “Group Policy Fundamentals.” We then expand on how to control different aspects of GPOs, especially the inheritance of GPOs within Active Directory. You get these details in “Controlling GPO Inheritance.” Then, we move on to discuss the fact that there are plenty of default settings, GPOs, and access points built in to the interface and domain. We go over what each shortcut and setting controls, so you know what you’re getting out of the box. We cover this in “Default GPOs and their Shortcuts.” The final section, “Key Group Policy Configurations,” gives you insight into some of the more complex, yet important, configurations within a GPO.
Group Policy Fundamentals

What Is a GPO?

A GPO is a group of settings. The name Group Policy Object is somewhat confusing, if you attempt to use the words in the term to try to figure out what it does. Some call a GPO a “group of policy settings” or a “group of policies.” This more closely represents what it actually is. The word “object” on the end of the term isn’t all that confusing, until you try to figure out how an object in Active Directory can configure other objects in Active Directory.

I like to think of a GPO as a set of rules that configure “like” computers or users. An example would be that all computers in the human resources (HR) department have the same security settings. The optimal way to implement the same security settings on these HR department computers is to use a GPO.

Another aspect of a GPO that is important to understand is that it is meant to automate the settings of a computer. Most of the settings that control the desktop, security and applications within a GPO can be done manually. It is just that the GPO does all of this work automatically for the administrator. Some settings like service access control lists (ACLs) and detailed IP Security configurations are harder to configure manually, so the GPO is just about the only method for configuring these settings.

What Does a GPO Do?

The settings within a GPO control a variety of different areas within a computer. As you investigate the structure of a GPO, you can clearly see the different areas that it affects. Some settings update the Registry, some configure files on the target computer, some modify operating system
variables, and other settings control protected areas of the operating system.

All of the different areas of a GPO will modify the target computer settings automatically. These settings from the GPO are initially applied to the computer when the computer is started and when the user logs on. The benefit to this strategy is to have the settings in place before any activity occurs, so that the environment can be established and secured before the user starts to work.

From the users’ standpoint, they don’t see much of anything going on. The logon screens show that things are happening, but it is really just a waiting period for the users. When users receive their desktops, all of the settings have been applied based on the rules the administrator configured in the GPOs.

**What Can a GPO Do?**

It might be easier to ask the question, “What can’t a GPO do?” A GPO can configure many different aspects of a computer or user environment. Each area is broken down into categories in the GPO interface. This allows you to configure each setting logically, independently and effectively. The following is the list of areas that are controlled by a GPO:

- *Application management.* Deploy, manage, update, control, and remove software applications on individual computers, or for specific users within the domain. GPOs can either use MSI or ZAP packages to deploy software. This can be configured for both a User and Computer object.

- *Disk Quotas.* These control how much data a user can store on a volume located on a server. Although this setting can’t control the detailed configurations on the volume, it does control whether or not disk quotas can be used. Disk quotas are configured for Computer objects only.
• **EFS Recovery.** Encrypting File System (EFS) provides the ability for users to encrypt data stored on servers. After encryption, only a narrow set of users can access the data. By default it’s only the user that performed the encryption. To recover from a problem with this limited access, the EFS Recovery agent can decrypt the data. EFS Recovery agents are configured for Computer objects only.

• **Folder Redirection.** This provides an outlet for administrators to redirect folders typically stored on the local computer of a user. The redirection is to a central server, so the data can be secured and backed up regularly. There are a limited number of folders that can be redirected: the Application Data from the user’s profile, the Desktop, My Documents, and the Start Menu. Folder redirection is only available for User objects.

• **Internet Explorer Settings.** IE has numerous settings that need to be configured for secure and efficient Internet access. This includes Security Zones, Proxy Server settings, URL Favorites, etc. All of these settings and more can be completed via GPOs. Both Computer and User objects have IE policy settings.

• **IP Security.** This encrypts data that is sent over the network, from the source to the target. The IP Security settings provide detailed control over how the security will be implemented. IP Security settings are only available for Computer objects.

• **Registry Settings (Administrative Templates).** Almost every Registry setting can be controlled through GPOs. This spans Internet Explorer, Desktop settings, Start Menu, and more. The default Administrative Templates configure a broad range of settings, but can also be customized to meet almost any setting. Both Computer and User objects can be controlled with Administrative Template settings.
• **Scripts.** There are four different types of scripts through GPOs. Startup and Shutdown scripts are associated with a computer being turned on or off. Logon and Logoff scripts are associated with a user logging on or off the domain. Almost any task can be performed through a script, including establishing network printers, mapping network drives and scheduling tasks.

• **Security.** Security in a GPO spans authentication, network access, logon, secure communication and more. There are settings for both Computer and User objects, but the majority of the security-based settings are for the Computer objects.

As you can see, there are numerous areas that a GPO can affect. All in all, there are almost a thousand GPO settings throughout these areas. Combine that with the almost endless customization options that apply to any GPO and you can see that GPOs are extremely powerful, plus highly complicated.

**The GPO v. System Policy**

If you’re coming from a Windows NT domain, it is important to understand the differences between the old style System Policy and the new GPOs in Windows Active Directory. The changes seem subtle, but in reality they’re quite different.

**System Policy**

To start off, let’s review quickly what an old world System Policy consists of:

• There is only one System Policy per domain.

• The System Policy was at the domain level, affecting all objects in the domain by default.
• The System Policy is stored in the NETLOGON share on the domain controllers.

• The System Policy is named ntconfig.pol.

• The System Policy can affect user, computer and group accounts.

• The System Policy can be customized with ADM templates.

• System Policies are only applied at startup for computers and logon for users.

• All System Policy settings “tattoo” the Registry.

• The only settings that were included in a System Policy were for the Registry.

• To edit a System Policy, you would run the POLEDIT.EXE command.

Group Policy Objects

In comparison, GPOs have the following characteristics:

• There can be numerous GPOs.

• GPOs can be applied at the Site, Domain and OU levels with Active Directory. There is also a GPO at the local level for all computers that run Windows 2000 or higher.

• GPOs are stored in both SYSVOL and Active Directory.

• GPOs store GPOs with a complex array of files and folders.

• GPOs can only affect user and computer accounts.
• GPOs can be customized with ADM templates, security templates and modifications to the security settings with a default GPO.

• GPOs are applied to computers at startup and users at logon. Also, both portions of the GPO are applied at a periodic refresh interval, as well as they can be applied by running a command on the target computer.

• Most of the GPO settings don’t “tattoo” the Registry.

• GPOs provide settings that modify the Registry, system variables, software installation and operating system settings.

• To edit a GPO, you run the GPEDIT.MSC or Microsoft Management Console.

**What’s Unique to a GPO**

This is just a quick comparison of the overlapping areas that a System Policy and GPO have in common. However, there are many other areas that are unique to a GPO, which need to be configured in almost every environment to specify security and other settings on the computers in the environment. These special GPO settings include:

• *Account Policies.* Account Policies include Password, Account Lockout and Kerberos. These settings were moved to GPOs in Active Directory, whereas in Windows NT they were configured using the User Manager for Domains tool.

• *User Rights.* User rights control what a user can do on a computer. Many times user rights control servers. These settings were moved to GPOs in Active Directory, where in Windows NT they were configured using the User Manager for Domains tool.
• *Audit Policy.* Auditing provides tracking of security related events within the operating system. Auditing can be done on logons, account management, use of user rights and more. These settings were moved to GPOs in Active Directory, whereas in Windows NT they were configured using the User Manager for Domains tool.

• *Internet Explorer.* There is almost nothing you can’t control, configure and lock down in IE using GPOs. Although these settings were not part of the standard System Policy, they were an extension of the System Policy if you used the Internet Explorer Administration Kit (IEAK).

• *Security.* Many of the security related Registry modifications that were used in Windows NT domains were moved to GPOs. These settings now allow the control of network access, local access, authentication, and more to all computers in the Active Directory domain.

Other settings unique to a GPO aren’t even available in NT. Settings like Software Installation, IP Security, Certificates, Encrypting File System, and Remote Installation Services provide even more flexibility and capabilities to a GPO, whereas the System Policy was not capable of supporting such settings.

**Where a GPO Can Reside**

One of the basics of understanding GPOs is to grasp where they can reside within the enterprise. Because there can be more than one GPO, keeping track of them can be a full-time job, unless you fully understand where they can be located. The term “reside” is really not the ideal choice of wording, but it is better than the actual term of “linking.”
GPO Link

The concept of a GPO link is rather simple, but difficult to comprehend because it is hard to see the links. Remember, a GPO is a “group of settings.” This “group of settings” is stored in the GPO structure. The GPO does not do anything by itself; it must be targeted to other objects before it can make any changes. So, in order for a GPO to target user and computer accounts, it must be “linked” to the objects that contain the user and computer accounts. In Active Directory, objects that contain user and computer accounts include sites, domains and organizational units (OUs).

Note: Granted, sites really don’t contain user and computer accounts, but considering the hierarchy of Active Directory, sites do contain these objects. In the same light, domains typically don’t contain user and computer objects directly, rather, user and computer objects are located in OUs, which are all under the domain level.

Here are some things to consider when working with GPOs and links:

- A GPO can exist without having any links. This will result in a GPO that has no effect on any object in Active Directory.

- A GPO can exist and have numerous links. However, there is still only one GPO in this case.

You might think about the GPOs themselves as living in a central location. The location is separate from any other objects in Active Directory. Then, when a GPO needs to affect user or computer accounts, it is linked to the OU where those accounts reside. If more user and computer accounts need to be affected by the GPO, a different link is created to another OU. This matrix of links is created to control what objects the GPOs affect.

To see a listing of where GPOs are linked to, you can go to the following path:

1. Open Active Directory Users and Computers.
2. Right-click on the **Domain Controllers** OU (you could pick another OU or the domain to get the same results) and select **Properties** from the menu.

3. Select the **Group Policy** tab in the **Domain Controllers Properties** window.

4. Click the **Add** button.

5. Select the **All** tab in the **Add a Group Policy Object Link** window.

6. Right-click on the GPO that you want to see the links for and select **Properties** from the menu.

7. Select the **Links** tab in the `<GPOname> Properties` window.

8. Click the **Find Now** button to show all of the links to the domain objects, as shown in Figure 1, below
Figure 1. You can see a listing of all of the links to a GPO from the Links tab on the Properties sheet of the GPO.

A key item to remember with regard to GPOs and links, is that if you go to a link and edit the GPO from that location, you’re really editing the GPO. This includes ACL settings and policy settings. For example, if you had a GPO linked to both the Sales OU and the Managers OU, you’d go to the Sales OU and see the GPO listed under the Group Policy tab on the Sales OU Properties sheet. If you selected the GPO and then selected Edit, you would be editing the GPO, not the link. Any changes made to the GPO here would be reflected in the GPO that is also linked to the Managers OU.

**What a GPO Affects**

Like many other aspects of the Microsoft environment, the naming of GPOs can be confusing. The name implies something to do with a
“Group.” Yet, actually, GPOs have little to do with groups at all. There are only two objects that a GPO can apply to: user accounts and computer accounts. Group Policy objects don’t apply to groups! You can see this in the interface of the GPO Editor. When you open up the GPO Editor, you see two major sections: Computer Configuration and User Configuration, as shown in Figure 2, below. If you burn a mental picture of this into your memory, it will go along way to understanding, implementing and troubleshooting GPOs.

![Group Policy Object Editor](image)

**Figure 2.** In the GPO Editor it’s clear that GPOs will only affect Computer and User accounts. There is no mention of group accounts within the GPO Editor.

Now that is it 100-percent clear and obvious that GPOs affect user and computer accounts only, we need to take our understanding one step further. The next concept is the fact that GPOs only affect objects that are in its path. What do I mean by “path”? Here path refers to objects that inherit the GPO, down through the Active Directory structure. Let’s look at an example. Assume there are two OUs, named Sales and Marketing, directly below the domain level. All of the user accounts are located in the default Users container and all of the computer accounts are located in the default Computers container. If a GPO that removes the Run Command from the Start Menu is linked to the Sales OU, which objects will be affected? The
answer is none. This example illustrates that if no object is in the path of the GPO, then no object is affected.

If we take the example one step further and link the GPO to the domain level instead of the Sales OU level, we have a completely different scenario. If this is the new structure, which objects would be affected? The answer here is that all of the user objects are affected. The reason is that all user objects are in the domain. They are all located in the Users container under the domain. Why did I not indicate the Computer objects were affected? The reason is that the Run Command is a User Configuration, not a Computer Configuration, as Figure 3 illustrates.

![Figure 3. GPO settings fall under either computer accounts or user accounts.](image)

**Basic GPO Functions**

When it comes to administering GPOs, you need to consider two basic functions. GPOs must be created first. This includes the administrator establishing the new GPO altogether, then making the desired configurations in the GPO. Then, the GPO must be linked to the site, domain or OU.
Creating a New GPO

Creating a new GPO is something that all administrators should have the ability to do. GPOs can cause widespread disasters if they’re not configured properly. By default, only the Administrator can create GPOs in Active Directory. For an Active Directory that doesn’t have the Group Policy Management Console (GPMC) installed, this is given to the Administrator by placing the account in the Group Policy Creator Owners group.

**Note:** The reason that the GPMC is mentioned here is that it offers some new features that the standard method of GPO administration does not. However, we aren’t going to focus on the GPMC in this book. Instead, we are focusing on the built-in method of administering GPOs here. In the next digital report, Advanced Group Policy Objects, we’ll go into the GPMC in full detail.

We need to be clear exactly what creating a GPO provides, compared to what most administrators do when they create a GPO. If you’re like most administrators, you open up ADUC and go to the OU where you want the new GPO. Then, on the **Group Policy** tab on the OU Properties sheet, you select the **New** button, as shown in Figure 4, below.
Figure 4. The New button on the Group Policy tab allows you to create new GPOs, as well as link them to the OU.

When you perform this act, you’re doing more than just creating the GPO; you’re also linking it to the OU. If you have not been given “Link GPO” permission, you won’t even have the New button available when you look on the Group Policy tab.

If the New button is no longer available, then how do new GPOs get created? The answer is somewhat convoluted. To create a new GPO without using the New button, you need to go a couple of steps past the Group Policy tab. Follow these steps to create a new GPO without linking it to an object:

1. Open Active Directory Users and Computers.
2. Right-click on the **Domain Controllers** OU (you could pick another OU or the domain to get the same results) and select **Properties** from the menu.

3. Select the **Group Policy** tab in the **Domain Controllers Properties** window.

4. Click the **Add** button.

5. Select the **All** tab in the **Add a Group Policy Object Link** window.

6. Select the [ ] to create a new GPO.

7. Provide a new name for the GPO.

   This method creates a new GPO, but it won’t link it to any object. If you want to see this, just right-click on the new GPO and select **Properties** from the menu. Then, select the **Links** tab in the property window for the GPO. Click the **Link Now** button to see that there are no links for the GPO.

**Linking an Existing GPO**

As we just saw, when you create a new GPO from the site, domain or OU, it is linked automatically to the object where the GPO was created. However, it isn’t always possible to do this, since many companies require separation of privileges when it comes to creating and linking GPOs.

   For the company that requires separation of duties or if there is just an existing GPO that needs to be linked to the site, domain or OU, there is an option to just link a GPO, instead of having to create a new one in conjunction with the link. In a nutshell, linking a GPO to an object is only available if the GPO exists.

   One of the more common delegation of administration tasks for Active Directory is linking GPOs. It is one of the standard tasks in the Delegation
Wizard. In order to delegate the linking of GPOs to a particular OU, follow these steps:

1. Right-click on the OU where the delegation of linking GPOs will be given.

2. Select the Delegation Control menu option.

3. Select the Next button at the Delegation of Control Wizard window.

4. Select the Add button on the Users and Groups page.

5. Select the group or groups that you want to have the ability to link GPOs to this OU.

6. Select the OK button.

7. Select the Next button.

8. Select the Manage Group Policy links check box.

9. Select the Next button.

10. Select the Finish button.

This will give the users in the group that were configured using the wizard the ability to link GPOs to this OU and the child OUs to this OU. This works out ideally for branch offices, divisions of the company that have local administrators and separation of privilege.

In this case, the users in the group will have the Add button available on the Group Policy tab, but won’t have the New button available. I refer to the Add and New button on the Group Policy tab, because it is common to use the Group Policy tab to link GPOs; but additional links can be made to a GPO by going into the Group Policy Properties sheet.
**GPO Precedence**

GPO precedence is an extremely important aspect of putting together a GPO design. If the precedence of GPOs isn’t taken into consideration, there is no telling what the result will be for the computer and user environment. You will quickly see that the precedence of GPOs will drive the GPO design, as well as the design of the OUs. Of course, we might as well go all the way and say that the design of the GPOs many times drives the entire Active Directory design.

There are four different areas that need to be addressed with regard to GPO precedence. First, we’ll talk about the hierarchy of the GPOs and in which order they apply to users and computers. We will then talk about the situation where there are multiple GPOs linked to a single site, domain, or OU. Next, if we have all of these GPOs and they have some order of precedence, what happens if two different GPOs have the same setting? Who wins the conflict? Finally, taking into account GPO precedence and GPO conflicts must result in an end state. So, we’ll tackle how this end state is determined as well as what you can do to help yourself design and troubleshoot for all GPO issues.

**LSDOU**

Before we talk about the precedence of GPOs, we must know all of the different locations that are considered when applying GPOs to computer and user accounts. There is always a local GPO to be considered. Every computer has a local GPO. By default, there is always a domain GPO, named the Default Domain Policy. This too must be considered. The other two locations that can have a GPO linked to it are the site and OU levels. So, all of these different locations consist of local, site, domain, and OU. The acronym we use to refer to all of these is LSDOU.

Therefore, if you have a GPO linked to the site, domain, and OU, you would need to consider all four locations in your design and result of the GPO on the target object. The order that GPOs apply starts with the local GPO. The site GPOs apply next, then the domain, and then the OUs. The
precedence is the last GPO to apply has precedence over the previous ones. This holds true all the way down the line of all of the GPOs too. So, the GPOs linked to the domain have precedence over the site and local GPOs. Figure 5 illustrates what GPOs at these locations might look like graphically.

![Diagram of GPO hierarchy]

**Figure 5.** How GPOs link hierarchically through the local computer, domain, and OUs.

From Figure 5, the following would be the order of the GPO application for XPPro1:

1. Local GPO
2. Default Domain Policy
3. HR_GPO

4. West_GPO

**GPOs within Site, Domain or OU**

Now that we understand that the local GPO applies first, followed up by the site, domain and finally the OU GPOs, we can move to the next level of GPO precedence. We don’t need to worry about the local GPO at this level, since there can only be one local GPO. However, there can be multiple GPOs linked to the site, domain and OU, so we must consider how the GPOs are applied. Figure 6 shows what this might look like.

![Figure 6. There can be multiple GPOs linked to any one OU or site or the domain.](image)
When you have a situation like this, you need to understand how the GPOs will be applied, which will indicate their precedence. Even though the text tells you clearly how the precedence works, it seems to be overlooked quite often by administrators. The text clearly states, “Group Policy Objects higher in the list have the highest priority.”

So, the way the precedence works is that the operating system will come in at the bottom of the list, then work its way up to the top of the list to apply the GPOs. You might think that the operating system does the opposite—starting and the top and working down—but this is where many administrators get tripped up.

The reason this is so important is that there are usually more than one GPO at any given level within Active Directory. It isn't often that two different GPOs have conflicting settings, but it is possible, which makes this discussion highly important.

To summarize, we now know that GPOs apply in the order of LSDOU. Within the SDOU structure, there can be multiple GPOs at any one level. At each level, the GPOs will be applied starting at the bottom of the list and working to the top.

**Appending and Conflicting Settings**

Now that we understand the precedence of GPOs from LSDOU and GPO ordering, we finally get to the finale. You might be wondering why we are even discussing GPO precedence at all. You might be thinking that your GPOs all have different GPO settings, which will append to one another to configure the user or computer account. And you would be partially correct. If you have 25 GPOs, all configuring different GPO detailed policy settings, then all of the settings will append to one another to apply to the user or computer account. Let's look at a small example.

Assume you have a user account located in an OU named HR. You have the local GPO on the Windows XP Professional computer configured to enable the “Remove Run menu from Start Menu” policy. Of course, this
will remove the Run command from the Start Menu. Then, you have a different GPO linked to the domain, which enables the “Remove Help menu from Start Menu” policy. This will remove the Help and Support option from the Start Menu. Finally, you have another GPO linked to the HR OU. This GPO disables the “Remove My Documents icon from Start Menu” policy. This will force the My Documents menu option to show up on the Start Menu. Figure 7 illustrates our GPOs and their settings.

![Diagram of GPOs and their settings]

**Figure 7.** When GPOs are at LSDOU locations, they append if there are no conflicts.

We can probably all agree that this summary of GPO settings is easy. However, this isn't as common as you might think. Most organizations have GPO settings that do conflict with one another as each GPO is applied. Granted, this isn't that common at the same level in the Active Directory structure, but from level to level, it is very common. Let's look at an example to get the full understanding of how conflicts are taken care of by the operating system.

Assume you have a user account located in the Benefits OU, which is a child OU to the HR OU. The local GPO on the Windows XP Professional computer is configured to disable the “Remove Run menu from Start
Menu” policy. This will add the Run command to the Start Menu. Then, you have another GPO linked to the domain, which enables the “Remove Run menu from Start Menu” policy. This will remove the Run command from the Start Menu. Then, you have a different GPO linked to the HR OU. This GPO disables the “Remove Help icon from Start Menu” policy. This will add the Help and Support menu option to the Start Menu. Finally, you have a GPO linked to the Benefits OU. This GPO enables the “Remove Help icon from the Start Menu” policy. This will remove the Help and Support menu option from the Start Menu. Figure 8 illustrates our GPOs and their settings.

Figure 8. When GPOs conflict, the last GPO applied wins.

This only illustrates the conflicts that can arise from GPOs at different levels. Conflicts can arise from GPOs that are located at the same level, such as the same OU. Good designs don’t have these conflicts, and you should take precautions to not force these types of issues.
Resultant Set of Policies

Whether you noticed it or not, we have already touched on this topic slightly. In the last section when we were dealing with GPO application and conflict resolution, the graphics hinted at the concept of Resultant Set of Policies, or RSoP as it is commonly referred. The RSoP is the final set of policies that apply to either the user or computer account. In the days of Windows 2000, this was a difficult thing to determine. As an administrator you could use tools like gpresult or FAZAM to help compile what the resulting policies were for a user or computer.

With the advent of Windows XP Professional and Windows Server 2003, the issues related to the RSoP aren't nearly as complex. To determine the RSoP now, you have a myriad of tools to assist you. Here are some of the tools that you have at your disposal to determine the RSoP for almost any situation:

- RSoP snap-in used with the Microsoft Management Console
- Help and Support Center
- Local Security Policy
- Group Policy Management Console

Figure 9 illustrates the Help and Support Center’s RSoP function.
Figure 9. Many tools can help determine the Resultant Set of Policies, which is essential for administrators to do “what-if” scenarios.

What exactly is the RSoP used for? If the GPOs aren't applying correctly to either the user or computer account, RSoP provides a way to determine what is applying to the different objects and from what location in the Active Directory. With hundreds of GPOs in a large organization, the RSoP is about the only way to determine what is applying on the target computer.
Note: I will cover RSoP and its related tools in depth in the third volume of this series, Troubleshooting Group Policy Objects.

GPO Application

Once the GPO is configured and you have the correct GPO precedence in place, it is now time to have the GPO take effect. Even though we would like to have this take effect immediately, that isn’t the case. GPOs take some time to get all the way to the target object, due to the technology that is driving them. Before we start to dive into the different technologies that are behind the GPO application, let’s take a quick trip back down memory lane to the world of Windows NT System Policies.

GPOs vs. System Policy Application

In order to appreciate the improvements that GPOs provide, we need to compare the GPO application process to the application of System Policies. GPOs are much different than their predecessor’s System Policies. A System Policy was limited to only applying to a user or computer at a new logon or restart, respectively. This was troubling and time consuming. The most annoying issue with the System Policies was that there was almost no way to force the user to log off or the computer to restart in order to get the policies to take effect.

Even though there was only one way to get a System Policy to apply, there are numerous methods to get GPOs to apply. The following is a list of ways that a GPO can be applied to a target object.

Computer:

- Restart computer.
- Wait for automatic refresh of GPOs.
- Manually force GPO application.
User:

- Log off and then back on.
- Wait for automatic refresh of GPOs.
- Manually force GPO application.

Of course, the GPOs must be on the correct domain controllers in order for any of these methods to be valid. The idea is that the GPOs must replicate from the domain controller that made the initial change to all other domain controllers in the domain. This will ensure that when the computer or user account attempts to apply the GPO, the domain controller has the latest and greatest GPO to apply. If the GPO has replicated, then the GPO application should be successful.

**More on Active Directory Replication**

Active Directory replication has two different forms: Intrasite and Intersite. Intrasite replication is when domain controllers replicate with other domain controllers in the same site. Intersite is replication between sites. Most large organizations have sites, so this is certainly something to consider. For Intrasite replication, the replication schedule is set to push changes between domain controllers every five minutes. This has a maximum convergence time of 15 minutes to all domain controllers in the same site.

For replication between sites, intersite replication, the schedule is much different. The default replication schedule is set to every three hours! This can be changed and many times is changed. Sometimes the change is to replicate less often, but usually it is set to replicate more often.

To calculate the maximum convergence time, you must consider the time the process will take to replicate in the site where the GPO was originally changed. Then, consider the time to replicate to the other site(s).
This might be tricky, depending on the site topology that you have implemented. Sometimes sites can be linked to one another, so you might need to take three hours and multiply it by the number of hops between sites. Finally, once the change is received on the destination site, there must be another calculation to accommodate the time needed to replicate to all domain controllers in the destination site.

All in all, this can total hours, maybe days. So, consideration of the site convergence for GPOs is extremely important when testing, implementing and troubleshooting GPOs.

**GPO Application to Computer Accounts**

As you investigate and learn how GPOs apply to target objects, make sure you consider which object you’re targeting. Here, we’ll talk about how GPOs apply to computer accounts, which is quite a bit different from user accounts.

Before you consider how the GPO will apply the target object, make sure you look at the correct object type. When you focus on a computer object, you’ll know for sure when you configure the “Computer Configuration” portion of the GPO, as shown in Figure 10.
After you configure the GPO, you have three options in order for the GPO to apply to the object as I mentioned earlier:

- Restart computer.
- Wait for automatic refresh of GPOs.
- Manually force GPO application.
Computer Account: Automatic Refresh

The default behavior for most organizations is to just let the default behavior for GPO application take its normal course. Unlike Windows NT System Policies, GPOs will automatically refresh the target computer at an interval of 90 minutes. This ensures that if any GPO change has occurred, it will show up on the target computer without any requirement of a restart or command line tool.

The refresh interval is every 90 minutes, but if all computers were trying to refresh at the exact same time, it would cause too much network traffic as well as punish the domain controller. Therefore, when the first refresh is determined, there is an offset of—at most—30 minutes, to get the computers staggered for their refresh schedule. The refresh will therefore begin with anywhere from 90 to 120 minutes.

Computer Account: Restarting Computer

This is a foolproof method to get a GPO to apply. If you’re ever stuck with getting a GPO to apply, use this method. Of course the reason you don’t want to use this method is that it takes a long time to restart the computer. (We aren’t talking about a logoff here; this is a complete restart of the operating system.)

When the computer restarts, you can see when the new GPO settings are applying in many cases, depending on what operating system you’re working with and what GPO setting is being applied. If you’re applying a lot of GPOs or a lot of GPO settings, the boot process might take a long time.

For some GPOs, it might take two restarts to get the settings to show up. This is due to how the GPOs work. For example, if you want to remove the username from the logon screen, this will take two restarts for it to show up. The first restart configures the Registry, but the Registry isn’t changed in enough time to show up when the logon screen appears. So,
after the second restart, the Registry setting is now correct, which will be indicated on the logon screen by not showing the last logged on user.

There are some settings that require this method of applying the policies. You won’t be able to auto refresh or manually apply them; you need to restart the computer for them to apply. These settings include:

- Software deployment.
- IPSec configurations.

**Computer Account: Manual Method**

Both the automatic refresh and restart methods aren’t horrible—they are just slow! If you want to see a faster application of the GPO settings, you can run a manual command against the target computer to get the GPO to apply immediately. The command differs between operating systems, although the outcome is identical.

For Windows 2000 computers, you’ll use the secedit.exe command. This is a built-in command that can be run from the command line. The syntax for applying a GPO to a computer account is as follows:

```
Secedit /refreshpolicy machine_policy
```

You can also throw in the /enforce switch, to push down ALL GPO settings, even those that are already applied to the computer.

If you’re running Windows XP Professional or Windows Server 2003, you have a much easier path. You can use the built-in tool gpupdate.exe. This tool is easier because there are no switches needed, you just run the following from the command line:

```
Gpupdate
```
Like the secedit command, you can include the /force switch to push down all GPO settings, even those that are already applied to the computer.

The gpupdate command will update both the computer and user portions of the GPO. So, if you want to target only the computer portion of the GPO, you can add some switches. This is typically not done, since the time to apply the computer and user settings isn’t much longer than just the computer, but the option is here nonetheless. If you want to target just the computer configuration, you would run the following command:

```
Gpupdate /target:computer
```

Another nice feature of the gpupdate command is that you can force the computer to restart, after the GPO is applied. This is required for a few of the GPOs that don’t apply until the computer is restarted. If you want to target only the computer object and have the computer restart automatically, you would run the following command:

```
Gpupdate /target:computer /boot
```

**GPO Application to User Accounts**

As I emphasized for the computer accounts, you need to make sure you’re looking at the correct object type for applying your GPO settings. When you’re focusing on a user object, you’ll know for sure when you configure the “User Configuration” portion of the GPO, as shown in Figure 11.
Figure 11. GPOs that target user accounts will have the User Configuration portion configured.

After you configure the GPO, you have three options in order for the GPO to apply to the object as we introduced above.

- Log off, then log back on.
- Wait for automatic refresh of GPOs.
- Manually force GPO application.
User Account: Automatic Refresh

Even for user accounts, the default behavior for most organizations is to just let the default behavior for GPO application take its normal course. GPOs for user accounts act the same as with computer accounts, in that they will automatically refresh the target user accounts at an interval of 90 minutes, ensuring that if any GPO change has occurred, it will show up on the target computer without any requirement of a restart or command line tool.

The automatic refresh isn't split between the computer and user portions of the GPO. The automatic refresh is for the GPOs as a whole. So, when the 90-minute refresh interval hits, both the computer and user portions will be applied.

User Account: Logging Off and Back On

If you want to ensure that all settings are going to apply regardless of the application method, then this is the method for you! Logging off and back on will ensure that the user portion of the GPO applies.

When the user logs back on, you can see when the new GPO settings apply in many cases by the logon window. Like the computer options, if you’re applying a lot of GPOs or a lot of GPO settings, the logon process might take a long time.

The user portion of the GPOs will also behave in such a way that it takes two logoff/logon cycles to get the setting in the Registry and on your screen. Also, some settings just don’t apply until the user logs off and back on. These would include:

- Software deployment
- Folder redirection
User Account: Manual Method

The user account GPO methods of auto refresh and logging off and on are much slower than just using the manual command line option. Like the computer command line, the commands are different depending on the operating system that you’re targeting the GPO at.

For Windows 2000 computers, you’ll use the secedit.exe command. This is a built-in command that can be run from the command line. The syntax for applying a GPO to a user account is as follows:

```
Secedit /refreshpolicy user_policy
```

You can also throw in the /enforce switch, to push down all GPO settings, even those that are already applied to the user.

If you’re running Windows XP Professional or Windows Server 2003, you have a much easier path. You can use the built-in tool gpupdate.exe. This tool is easier because there are no switches needed; you just run the following from the command line:

```
Gpupdate
```

Like the secedit command, you can include the /force switch to push down ALL GPO settings, even those that are already applied to the user.

If you want to target just the user configuration, you would run the following command:

```
Gpupdate /target:user
```

For the software deployment and folder redirection, you’ll need to log off and back on. The gpupdate command can automatically do this for you if you use the correct switch. If you want to target only the user object and have the user automatically log off, you would run the following command:
GPO Fundamentals Summary

As you can see, the fundamentals of GPOs aren’t as bad as it seems. Yes, GPOs can be complex, hard to configure, and difficult to troubleshoot; but if you break down the concepts into small bites, it is easy to figure out. With all of these fundamentals, there seem to be a couple of key concepts that get lost in the translation from theory to implementation. To help you keep track of these fundamentals, always remember the following concepts:

- GPOs inherit down through the Active Directory structure. This means that any GPO that is linked high in the Active Directory structure, such as the domain or a high level OU, will affect more objects than a GPO that is linked low in the Active Directory structure, such as a low level OU.

Example: If there is a computer account located in the Computers container, it would receive the settings configured in a GPO linked to the domain.

- GPOs only apply to user accounts and computer accounts. You can’t apply GPOs to groups!

Example: There is a group named Sales. Sales has two user accounts as members, Joe and Sally. Joe’s user account is located in the OU named Sales_staff. Sally’s user account is located in the Users container. There is a GPO linked to Sales_staff, which removes the Run command from the Start Menu. The GPO ACL is changed to only allow the Sales group permission to apply the GPO. When the GPO applies, it will only affect Joe, not Sally!

- GPOs can only apply to an object, if the object is located in the path of the GPO. This means that computer or user objects must be located in the OU where the GPO is linked. Couple this rule
with rule #1 and the computer or user account can also exist in a child OU and receive the GPO setting through inheritance.

**Example:** There are two OUs named AP and AR. Betty works in AP and has a user account in the AP OU. Tom works in AR and has a user account in the AR OU. The AP OU has a GPO named *All_accountants* linked to it. When the GPO applies, it will only affect Betty!

- GPOs can’t apply to computer and user accounts through group membership. Combining #2 and #3 from this list will get you to this #4 tip, but many administrators still try to have GPOs apply to accounts, based on group membership only. (This does not contradict the fact that you can “filter” on groups; this is stating that you can’t have ONLY the group in the OU and have the members of the group receive the GPO settings.)

  **Example:** See Example in #2.
GPO and Active Directory Design Considerations

Although this book isn’t written to be a design aide, there is almost no way to dodge the concepts of designing GPOs when you talk about the basics of GPOs. With any good design discussion, we need to discuss all of the considerations that need to go into the design and implementation.

To start, consider that most GPOs are linked to OUs. Yes, you can link GPOs to the domain and sites, but the majority, 90 percent-plus will be linked to the OUs. So, we need to consider the design of the OUs when we talk about the design of the GPOs. When considering the OU design, there are two main issues to keep in mind. One is for delegation of administration. The other is for GPO application. Many like to leave out the concept of GPO design when considering the OUs, but it is mandatory that you think about your GPOs during this time.

If you aren’t familiar with delegation of administration, think of it like this: It is the concept that you’re going to give other administrators, junior-level admins or help desk personnel a subset of privilege to the objects in an OU. The most common delegated task is the “Reset Password” permission. For example, assume you have an OU named HR that has all of the user accounts for the HR employees located in it. You want July, the HR Manager, to have the ability to reset passwords for all of the HR employees. To make this work, you give July the “Reset Password” permission for the HR OU. Since the permissions inherit down, it means that July can reset passwords for all HR employees. However, since July was only given privilege to the HR OU, she can’t reset the password for any other user in the domain.
Common OU Designs for GPOs

GPO design needs the consideration of “who” will get “what” configuration. Remember, the “who” can either be a computer or a user account. As you think about the OU design, consider some common examples of how you might want to organize and name your OUs for GPOs.

- **Server role (IIS, Exchange, SQL, etc.).** GPOs can easily configure services, so you might have a special OU for each server type. This will give you the opportunity to control which services are running on the servers. It might be to ensure a service always starts when the computer starts, or it might be that you want to ensure that services don’t start when the computer starts.

- **Client computers.** It is common to control many aspects of client computers—from the screen saver, to the location of the My Documents folder, to which applications are installed for each type of user. Some companies organize client computers into a single OU, where other companies might have a top-level “Client Computers” OU and child OUs for each department in the company. The computer accounts for each department will be located according to their department, and GPOs will be linked to the departmental OUs. There might also be a GPO linked to the “Client Computers” OU, which are the common GPO settings that need to affect all computers in the company.

- **IT Staff client computers.** I think it is fairly clear that the IT staff needs different security and functionality on their computers. For example, IT staff computers need to have the Run command, where typical employee computers don’t need that function. Another example would be the configuration of Internet Explorer. The IT staff typical is responsible for downloading applications and testing tools. In this case, IE would need to have download capabilities, where the typical user might not have this capability.
• **Developers.** Many times developers need to have special configurations on their computer, due to the applications they develop. Also, many developers need to have unique access to network resources, which might require special logon scripts to give them access to hidden network shares. The developer computer might give the developer’s user account local administrative privilege, which isn’t common for most other users in the company.

• **Service accounts.** Service accounts are user accounts in Active Directory. These accounts should not be subject to certain security or other restrictive GPO settings, due to their need to have administrative access to the application they are controlling or, in many cases, the server the application runs on.

• **Secured client computers.** If your company has kiosks, shared computers or computers that run applications that control essential company data, you might want to create a special OU for these computer accounts. This will allow you to control them more securely than other computers. You might also want to have these computers use different Software Update Service Server nodes to download the majority of the security updates from Microsoft.

• **HR Servers.** This is just an example of a specialized type of server that might need additional attention for security reasons. With the advent of IP Security, you can lock down a computer quite securely. However, you need to create special OUs for this, since many networks can have all computers using IP Security, due to compatibility and network overhead reasons.

• **Branch Office.** Depending on how your organization is administered and controlled, you might have a special OU for the Branch Office. This would include all client computers, user accounts, and servers for that office. You can then create an OU hierarchy to control how the GPOs are assigned, using some of
the other categories in this list. Many times the Branch Office has more limitations for IE, desktop, and network resources, because they are removed from the main office and the administrators that live there.

These are just some examples of what your OUs might look like. As you read over the examples, you can see that some of the OUs could also be used for delegation of administration purposes. There is usually quite a bit of overlap between delegation and GPO application, which provides for a reduction in the complexity of the overall OU and Active Directory design.

**Where To Link the GPO**

Even though GPOs are primarily linked to OUs, that does not rule out linking them to the sites and domain. There are usually distinct reasons for linking them or not linking them to these other objects. What follows are some rules of thumb concepts for why you might link GPOs to other objects in Active Directory.

**GPOs Linked to Sites**

It isn’t common to link GPOs to sites. By far, it is the least used feature from the LSDOU option list. However, there are some key benefits to linking GPOs to sites. Before we cover those benefits, let’s discuss the disadvantages first.

A key disadvantage to using GPOs that are linked to sites is the fact that most administration of security and control isn’t done site by site. If you think about what is involved in a site, you should envision client computers, servers and domain controllers. If you were to link a GPO to a site, all of these computers would be affected by the GPO linked to the site. This, of course, can cause some catastrophic results.

You could, however, use GPO filtering to help reduce the exposure to the effects of the GPO, but there are other design options to eliminate this
need. I will talk about GPO filtering shortly, but it is important for me to mention here. In short, GPO filtering is controlling what objects will receive the GPO settings.

On the benefit side, what good can come from linking a GPO to a site? There are a couple of solutions that are fairly common. First, you can use GPOs linked to sites to control your “remote access clients.” This is a good idea, since most remote access solutions have a dedicated network of IP addresses for the dial-up and VPN clients. Here, you can lock down these clients with more robust security settings. You can also direct them to a shorter list of network shares, which will reduce your exposure from the outside networks.

The other use for GPOs at the site level is for directing client computers to the local Software Update Service (SUS), or Windows Update Service (WUS). (These are the same technology, but at the time of this writing, Microsoft was just making the switch from SUS to WUS).

If you aren’t familiar with WUS, it is the option to have a localized server function as the Windows Update Service from Microsoft. The idea is to have the local server deliver the updates, which are first approved by the administrator. It isn’t a good idea to have users attempting to download and install updates from the Internet, due to compatibility and security issues.

With the GPO linked to the site, you can control which WUS server the client computer and server use to receive their updates. This is ideal since the updates can be large, and you want to direct the client computers and servers to a local WUS server, not one that is located across the network or WAN.

**GPOs Linked to the Domain**

The domain has a default GPO linked to it, but the GPO that is linked to the domain does not configure much more than the Account Policies. The
reason for this is the same reason that it is so hard to link GPOs to sites. A GPO linked to the domain will affect every computer or user account.

This isn’t just a couple of computer and user accounts; by default this would include every single account. From my experience, there are only a few GPO settings that can survive at the domain level. Some of the settings include:

- Screen saver.
- Screen saver password timeout.
- Internet Explorer settings.
- IP Security configurations.

Beyond this list, the settings need to differ for different computer types and user types. Like the example with the site GPOs, there are too many different types of objects to have such a wide sweeping effect on the objects.

**GPOs Linked to OUs**

This is where Active Directory shines in regards to GPOs. When a GPO is designed along with the OU design, the power of the GPO can be used to the fullest extent. There is only one OU by default, and it has a default GPO linked to it. The Domain Controllers OU has the Default Domain Controllers Policy linked to it. This GPO primarily configures the User Rights for the domain controllers, but you can see how important a GPO linked to an OU can be.
Controlling GPO Inheritance

By default GPOs inherit down through the Active Directory structure. Also remember that the locations and application order that GPOs adhere to play a key role in the inheritance and Resultant Set of Policies on the target object. Experience shows that most companies take full advantage of the built-in inheritance that GPOs exhibit. Most purists (like me) feel that 99 percent of all GPO applications can be designed into the OU design.

The other one percent of the GPO design just won’t fit into the Active Directory design, due to a limitation of the delegation of administration design considerations. When there is a conflict between delegation or GPO application, the delegation will win most often. The reason for this is that delegation can only be accomplished one way. GPOs can either use inheritance, or you can break the inheritance and control what objects in the path of the GPO will receive the settings.

Breaking the inheritance of GPOs is a rather hefty task. Not that the breaking step is that tough, but if anything needs to be fixed due to an incorrect setting, configuration or otherwise, it can take a long time to track down where the inheritance starts and stops. For these reasons, it is recommended that you do not use any inheritance-altering methods, unless there is an absolute need.

There are three common methods used to break the inheritance of GPOs:

- Block Inheritance
- No Override
- ACL Filtering
Each setting has a slightly different approach and result, but all are effective in changing the default GPO inheritance behavior.

**Block Policy Inheritance**

The first method we’ll investigate is the option to block policy inheritance. This method does exactly what you would think it would, based on its name: It blocks all policy inheritance. The big question is where does it block the policy inheritance?

Block policy inheritance is a setting that can be configured on an OU and at the domain level. The local computer can’t block policy inheritance, since it is the first one to apply. There would be nothing to block. The site level would only be blocking the local GPO, if that were possible. However, it isn’t possible for the site level to block policy inheritance.

If you’re using the default GPO interfaces to administer GPOs, the setting to block policy inheritance is located on the Group Policy tab for the object properties of the site, domain, or OU where the GPO is linked. You can see this in Figure 12, below.
Think of block policy inheritance as a “shield” that blocks all GPOs that would apply to the domain or OU. For example, if there were an OU named Sales that had the block policy inheritance configured, it would block the local GPO, the site GPOs, and the domain GPOs. Then, the GPOs configured on the Sales OU would apply. These GPOs would then be the only ones to continue along the Active Directory structure, all the way down to where the objects reside.

In the graphical representation in Figure 13 you can see that there is a configuration on the West OU that is blocking the policy inheritance.
We learned earlier that the default inheritance for this configuration would be:

- Local GPO
- Default Domain Policy
- HR_GPO
- West_GPO

XPPro1 computer would receive the resultant set of policies that all of the GPOs develop. However, Figure 13 blocks the standard inheritance,
which alters the normal flow and application of the GPOs. The new result would be the application of the following GPOs on XPPro1:

- Local GPO

- West_GPO

Notice that the Local GPO can’t be blocked. Another point to notice is that the Default Domain Policy is being blocked, which is where the Account Policies are configured. This is an important factor, since most companies rely on the Account Policies at the domain level to control not only the domain user accounts, but also the local SAM accounts on all domain members.

If you’re an administrator in control of the overall security and configuration of your enterprise, you might be concerned at this point. This example illustrates the power that a junior-level admin can have, if given power over the GPOs in any way. Imagine that you have delegated administrative privilege to a junior admin at the West OU level. With the right permissions, the admin with delegated privilege could configure this inheritance block. You, as the enterprise administrator, would not be aware of the change until it was too late. The most likely way you would find out about the change is that a computer would be attacked, because the security configurations you had implemented at the domain or HR OU level would be blocked.

**No Override**

If you’re a “worried” administrator, this section is for you. The block policy inheritance setting can cause problems for administrators higher in the Active Directory, because the block policy inheritance setting does not show up anywhere in the interface, but on the object (domain or OU) where it is configured.

I had a boss once who used to say, “If you have tried to fix it, but it is still broke, get a bigger hammer!” Although this way of thinking has
caused me some grief over the years, the saying works here. If administrators lower in the Active Directory hierarchy are causing problems by configuring block policy inheritance, then you, as the higher level administrator, can use the no override setting to fix the problem. Yes, no override is a “bigger hammer” than block policy inheritance, because it ignores any blocked configurations.

Figure 14 illustrates what a configuration of no override might look like graphically.

![Diagram](image)

**Figure 14.** No override can be applied at the site, domain or OU levels. No override ignores block policy inheritance settings.

No override is a “per GPO setting,” which can be configured at any level in the Active Directory structure. However, no override can't be configured at the local GPO level. In our example in Figure 14, we can
remember what the GPO settings were for XPPro1 when just the block policy inheritance setting was in place:

1. Local GPO

2. West_GPO

Now, with the no override setting configured at the HR_GPO, the new set of policies that will affect XPPro1 are:

1. Local GPO

2. HR_GPO

3. West_GPO

The no override setting on the HR_GPO has more effect than just forcing its way down the Active Directory hierarchy. When the setting is made on a GPO for no override, it also specifies that the settings in the GPO can't be changed by a different GPO that has a higher precedence.

So, if the HR_GPO removes the Run command from the Start Menu and the West_GPO adds the Run command to the Start Menu, the no override setting on the HR_GPO will enforce the removal of the Run command from the Start Menu. This contradicts the standard GPO inheritance and precedence order, but it is necessary when junior administrators have free reign over GPOs and settings lower in the Active Directory structure.

To configure the no override setting for a GPO at a SDOU level, you access the Group Policy tab on the site, domain or OU property sheet, as shown in Figure 15, below.
Figure 15. No override can be applied at the site, domain or OU levels. No override ignores block policy inheritance settings.

Even though no override is a great feature, with plenty of power, it should be used sparingly. Instead of fearing that a junior administrator will cause problems, my suggestion is to just not give them the power to make these configurations to GPOs lower in the Active Directory structure. Like the block policy inheritance feature, the no override settings are difficult to track and see in the interface. Even though they control lower-level GPO settings, they only show up at the level at which they are configured.

**GPO Permission Filtering**

The concept of GPO filtering is simple. An object must have permission to apply the GPO. GPO permission filtering is done by altering the ACL on
the GPO itself. Think of GPO filtering just like you do controlling access to a file.

If you want to access a file, you need permission to the file. For example, assume you want to be able to modify data contained in a file. If you only had Read permission, you could not actually change the data in the file. Instead, you would need to have both Read and Write permission. The same concept applies to GPOs. In order to have a GPO affect a user or computer account, the target object needs to have both Read and Apply Group Policy permission. By default, this is accomplished by having the Authenticated Users group on the ACL possess these permissions. Of course, all user and computer objects have membership in this group.

Keep in mind that the Authenticated Users group includes all User accounts and Computer accounts. This would include all administrator user accounts too, even the built-in default Administrator account.

Every object in the path of the GPO will receive the settings in the GPO by default, due to the Authenticated Users group. Well, what if you want all but a few objects to receive the GPO settings? Of course, you could always move the account from the OU, but there might be four other GPOs at the OU that the account needs. This is where we use the concept of GPO Filtering.

Since objects need both Read and Apply Group Policy in order to apply the GPO settings, all you need to do is take away one of these permissions for the object and it won’t apply the GPO. Let’s look at a quick example:

There are three user accounts in the HR OU: Joe, Betty and Sally. There is a GPO linked to the HR OU. The GPO configures the Start Menu to remove the Run Command. However, you realize that Sally needs to have the Run Command, and you need her in this OU for delegation of administration. So, you have a user account in the OU that should not have the ability to apply the GPO for the Run Command.
To continue with our example, we need both Joe and Betty to get the GPO, but not Sally. So, we add Sally to the ACL and Deny/Apply Group Policy for her user account. When the permissions are being calculated for Sally, she won’t get the permission to apply the GPO, so she will end up having her Run Command.

**Note:** I could also add Sally to a group and add the group to the ACL, configuring the group to have Deny/Allow Group Policy permission.

There is great power in the use of the Authenticated Users having both Read and Apply Group Policy permission. You need to use this power to your benefit. For example, if you want a GPO to apply to all users in an OU, except for a small group, it is best to leave the default Authenticated Users on the ACL. Then, just add in the small group to the ACL, denying them the ability to Read the GPO.

On the other hand, the Authenticated Users is a broad stroke, which can cause some unpleasant behavior with the application of GPOs, if you aren’t careful. Say, for example, you want only the IT group to apply a GPO. Including the Authenticated Users on the ACL can create an abundance of settings for the computers and user accounts in the path of this GPO. Ideally, you want to remove all user and computer accounts that could receive the GPO from the ACL, but this can cause an abundance of GPO settings. Instead, it is best to remove the Authenticated users group from the ACL, which will at first glance give no one access to the GPO. The final step for this method is to add in the IT group only the ACL of the GPO that they will need to receive. The final result is that all Members of the IT group will receive the GPO, but no other user account will, even if it is located in the path of the GPO. This is because it lacks both required permissions to apply GPOs.

GPO filtering is a complex and difficult aspect of GPOs. However, when used appropriately, it can be useful. When you do use GPO filtering, there are some minor points to keep in mind:
1. The ACL for a GPO is on the GPO itself, not the GPO Link to the Site, domain or OU. If a single GPO is linked to multiple objects in Active Directory, a change to the GPO ACL at one level will change the GPO ACL at all levels.

2. GPO filtering can be difficult to troubleshoot, since there is no way to look at the inherited permissions for the GPOs.

3. Designing your OUs for GPO application should be one of the key design criteria for all OUs. However, there might be a cause for GPO filtering. If you can design the OUs within the Active Directory design for application of GPOs, there will be no need for GPO filtering, which can be good! Use GPO filtering sparingly.

**GPO WMI Filtering**

A new GPO feature with Windows Server 2003 is the use of WMI filtering to target specific computers. The WMI filter is a query that is attached to a GPO. The filter will return all computers that fulfill the query requirements. The computers that fulfill the requirements will then receive the GPO settings.

Most queries use the Root/CMIV2 class. The language for WMI is similar to SQL, and is called WQL language.

WMI is an acquired skill, but if you have been working with scripts or doing software development, WMI scripts will come easily. However, if you need guidance or assistance, you can use the Scriptomatic tool! The tool is available from the TechNet scripting center and is called scriptomatic.hta. A tip in using the tool is to reference the Win32_operatingsystem category, which contains most of the variables that you’ll use to query computers.

Also, when you create your script, you’ll use Boolean operators to help control what you’re querying. When you want to gather computers in a
general form, you’ll use the LIKE operator. When you want to gather computers that meet a detailed criteria, you’ll use the = operator.

This example will walk you through how to create and tie a WMI filter to a GPO. In this WMI filter, we’ll query only the Windows XP Professional operating system computer accounts. If the computer account is running anything other than Windows XP Professional, it won’t receive the GPO settings that are tied to the WMI filter.

We first need to establish where we want to have the WMI filter located. We are going to focus on the HR department computers. The HR department in our example has an OU directly under the domain, and it is named HR. There are both user and computer accounts directly under the HR OU. There is an existing GPO that is linked to the HR OU, which configures some of the new GPOs that only target Windows XP Professional computers. This is why we want to create a WMI filter, to target the XP computers.

To create the WMI filter, we need to go to the GPO that is linked to the HR OU and access the properties of the GPO. Follow these steps to get to this point:

1. Right-click on the HR OU and select **Properties** from the menu.

2. Select the **Group Policy** tab on the HR Properties window.

3. Select the **GPO** from the list and select the **Properties** button.

4. Select the **WMI Filter** tab on the HR Properties window.

5. Select the “**This filter**” radio button and select the **Browse/Manage** button.
6. Select the **Advanced** button on the Manage WMI Filters window.

7. Select the **New** button.

8. Type in **XP Pro Only** into the Name field.

9. Type in **Root\CIMV2; SELECT * FROM Win32_OperatingSystem WHERE Caption LIKE “Microsoft Windows XP”** in the Queries text area.

10. Select the **Save** button.

11. Select the **OK** button.

12. Select the **OK** button on the HR Properties window.

13. Select the **OK** button on the next HR Properties window.

   The WMI filter is now in place and will only target Windows XP Professional computers.
Default GPOs and Their Shortcuts

Every Active Directory domain has two default GPOs. These GPOs establish the security for the user accounts and the domain controllers. Access to these GPOs can be a bit confusing, since there seems to be many ways to access them. In some cases, the links to the GPOs only give you a partial listing of what is included, instead of the full access and list of settings. In this section, I explain the default GPOs and the links that are available to access them.

Default GPOs

No matter how you get to Active Directory, you’ll have two default GPOs. Both have their uses and are very much needed. It is my suggestion, as well as the suggestion of Microsoft, to not delete these default GPOs.

One of the GPOs is linked to the domain level and the other is linked to the Domain Controllers OU. They’re named according to what their scope is. The GPO linked to the domain is named Default Domain Policy, and the one linked to the Domain Controllers OU is named Default Domain Controllers Policy.

Each GPO has a distinct function, as well as default settings. Let’s look at each GPO and its default settings.

Default Domain Policy

This GPO has a single primary function: to configure the Account Policies for all domain users. Remember, the Account Policies include: Password, Account Lockout and Kerberos. This setting is a computer setting, and it configures the domain controllers to control all domain user accounts. Since it is located at the domain level, it will also configure the local SAMs of all domain members, as long as a GPO at an OU does not conflict and change the settings.
Figure 16 shows the Default Domain Policy regarding the Account Policies.

![Group Policy Object Editor](image)

**Figure 16.** Account Policies in the Default Domain Policy.

The Default Domain Policy does more than just specify the Account Policies. Table 1 shows a list of the default settings in the Default Domain Policy.

**Table 1.** Default Domain Policy default configurations and values.

<table>
<thead>
<tr>
<th>Computer Configuration</th>
<th>Policy Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Policy</td>
<td>Enforce Password History</td>
<td>24 passwords remembered</td>
</tr>
<tr>
<td></td>
<td>Maximum Password Age</td>
<td>42 days</td>
</tr>
<tr>
<td></td>
<td>Minimum Password Age</td>
<td>1 day</td>
</tr>
<tr>
<td></td>
<td>Minimum Password Length</td>
<td>7 characters</td>
</tr>
<tr>
<td></td>
<td>Password must meet complexity requirements</td>
<td>Enabled</td>
</tr>
<tr>
<td></td>
<td>Store passwords using reversible encryption</td>
<td>Disabled</td>
</tr>
<tr>
<td>Account Lockout Policy</td>
<td>Account lockout duration</td>
<td>Not Defined</td>
</tr>
<tr>
<td></td>
<td>Account lockout threshold</td>
<td>0 invalid logon attempts</td>
</tr>
<tr>
<td></td>
<td>Reset account lockout counter after</td>
<td>Not Defined</td>
</tr>
<tr>
<td>Kerberos Policy</td>
<td>Enforce user logon restrictions</td>
<td>Enabled</td>
</tr>
<tr>
<td></td>
<td>Maximum lifetime for service ticket</td>
<td>600 minutes</td>
</tr>
<tr>
<td></td>
<td>Maximum lifetime for user ticket</td>
<td>10 hours</td>
</tr>
<tr>
<td></td>
<td>Maximum lifetime for user ticket renewal</td>
<td>7 days</td>
</tr>
<tr>
<td></td>
<td>Maximum tolerance for computer clock synchronization</td>
<td>5 minutes</td>
</tr>
<tr>
<td>Local Polices\Security Options</td>
<td>Network security: Force logoff when logon hours expire</td>
<td>Disabled</td>
</tr>
<tr>
<td>Public Key Policies</td>
<td>Encrypting File System</td>
<td>Administrator is configured as a Data Recovery Agent</td>
</tr>
</tbody>
</table>
The User Configuration portion of the Default Domain Policy isn’t configured for any setting.

**Default Domain Controller Policy**

The Default Domain Controllers Policy GPO is linked to the only default OU, which is the Domain Controllers OU. This GPO provides some essential security for the domain controllers, including security settings, User Rights, and Audit Policy. The primary focus is on the User Rights for the domain controllers, as shown in Figure 17, below.

![Group Policy Object Editor](image)

**Figure 17. User Rights Assignment in the Default Domain Controller Policy.**

The Default Domain Controller Policy does more than just configure the User Rights for the domain controllers. Table 2 shows a list of the default settings in the Default Domain Controller Policy.

**Table 2. Default Domain Controller Policy default configurations and values. Note: User Rights not filled in are either not defined or are defined but are left empty.**

<table>
<thead>
<tr>
<th>Computer Configuration</th>
<th>Policy Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Policy</td>
<td>Audit account logon events</td>
<td>Success</td>
</tr>
<tr>
<td></td>
<td>Audit account management</td>
<td>No auditing</td>
</tr>
<tr>
<td></td>
<td>Audit directory service access</td>
<td>No auditing</td>
</tr>
<tr>
<td></td>
<td>Audit logon events</td>
<td>Success</td>
</tr>
<tr>
<td></td>
<td>Audit object access</td>
<td>No auditing</td>
</tr>
<tr>
<td></td>
<td>Audit policy change</td>
<td>No auditing</td>
</tr>
<tr>
<td></td>
<td>Audit privilege use</td>
<td>No auditing</td>
</tr>
<tr>
<td></td>
<td>Audit process tracking</td>
<td>No auditing</td>
</tr>
<tr>
<td>User Rights Assignment</td>
<td>Action Description</td>
<td>Permissions</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Audit system events</td>
<td>No auditing</td>
<td></td>
</tr>
<tr>
<td>User Rights Assignment</td>
<td>Access this computer from the network</td>
<td>Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS, Everyone, Pre-Windows 2000 Compatible Access</td>
</tr>
<tr>
<td>Add workstations to the domain</td>
<td>Authentication required</td>
<td>Administrators, LOCAL SERVICE, NETWORK SERVICE</td>
</tr>
<tr>
<td>Adjust memory quotas for a process</td>
<td>Authentication required</td>
<td>Administrators, LOCAL SERVICE, NETWORK SERVICE</td>
</tr>
<tr>
<td>Allow logon locally</td>
<td>Authentication required</td>
<td>Account Operators, Administrators, Backup Operators, Print Operators, Server Operators</td>
</tr>
<tr>
<td>Back up files and directories</td>
<td>Authentication required</td>
<td>Administrators, Backup Operators, Server Operators</td>
</tr>
<tr>
<td>Bypass traverse checking</td>
<td>Authentication required</td>
<td>Pre-Windows 2000 Compatible Access, Administrators, Authenticated Users, Everyone</td>
</tr>
<tr>
<td>Change the system time</td>
<td>Authentication required</td>
<td>Administrators, Server Operators</td>
</tr>
<tr>
<td>Create a pagefile</td>
<td>Authentication required</td>
<td>Administrators</td>
</tr>
<tr>
<td>Debug programs</td>
<td>Authentication required</td>
<td>Administrators</td>
</tr>
<tr>
<td>Deny access to this computer from the network</td>
<td>No access</td>
<td>&lt;domain&gt;\Support_*</td>
</tr>
<tr>
<td>Deny log on locally</td>
<td>Authentication required</td>
<td>&lt;domain&gt;\Support_*</td>
</tr>
<tr>
<td>Enable computer and user accounts to be trusted for delegation</td>
<td>Authentication required</td>
<td>Administrators</td>
</tr>
<tr>
<td>Force shutdown from a remote system</td>
<td>Authentication required</td>
<td>Administrators, Server Operators</td>
</tr>
<tr>
<td>Generate security audits</td>
<td>Authentication required</td>
<td>LOCAL SERVICE, NETWORK SERVICE</td>
</tr>
<tr>
<td>Increase scheduling priority</td>
<td>Authentication required</td>
<td>Administrators</td>
</tr>
<tr>
<td>Load and unload device drivers</td>
<td>Authentication required</td>
<td>Administrators, Print Operators</td>
</tr>
<tr>
<td>Log on as a batch job</td>
<td>Authentication required</td>
<td>&lt;domain&gt;\IIS, &lt;domain&gt;\UUSR, &lt;domain&gt;\IWAM, &lt;domain&gt;\Support_*, LOCAL SERVICE</td>
</tr>
<tr>
<td>Log on as a service</td>
<td>Authentication required</td>
<td>NETWORK SERVICE</td>
</tr>
<tr>
<td>Manage auditing and security log</td>
<td>Authentication required</td>
<td>Administrators</td>
</tr>
<tr>
<td>Modify firmware environment variables</td>
<td>Authentication required</td>
<td>Administrators</td>
</tr>
<tr>
<td>Profile system performance</td>
<td>Authentication required</td>
<td>Administrators</td>
</tr>
<tr>
<td>Remove computer from docking station</td>
<td>Authentication required</td>
<td>Administrators</td>
</tr>
<tr>
<td>Replace a process level token</td>
<td>Authentication required</td>
<td>&lt;domain&gt;\IWAM, LOCAL SERVICE, NETWORK SERVICE</td>
</tr>
<tr>
<td>Restore files and directories</td>
<td>Authentication required</td>
<td>Administrators, Backup Operators, Server Operators</td>
</tr>
<tr>
<td>Shut down the system</td>
<td>Authentication required</td>
<td>Administrators, Backup Operators, Print Operators, Server Operators</td>
</tr>
<tr>
<td>Policy Area</td>
<td>Setting</td>
<td>Status</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Local Polices\Security Options</td>
<td>Take ownership of files and other objects</td>
<td>Administrators</td>
</tr>
<tr>
<td>Domain controller: LDAP server signing requirements</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Domain controller: Digitally encrypt or sign secure channel data (always)</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>Microsoft network server: Digitally sign communications (always)</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>Microsoft network server: Digitally sign communications (if client agrees)</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>Network security: LAN Manager authentication level</td>
<td>Send NTLM response only</td>
<td></td>
</tr>
</tbody>
</table>

The User Configuration portion of the Default Domain Controller Policy isn't configured for any setting.

**Account Policies Break the Rule**

The account policy settings are unique within GPOs, in that the account policies break the default inheritance and precedence model I’ve been talking about in earlier chapters. I don’t want you to think that all account policies break the standard rules; it is just one specific instance of the account policies.

The instance where this occurs is at the domain level, where the Default Domain Policy configures the account policies for all domain users.

Remember that GPOs follow the LSDOU rule for all inheritance and policy application priority. Not so with regard to the account policy setting for domain controllers. Remember the following and you won’t get confused again.

1. All domain user accounts’ account policy settings are controlled by the account policy settings configured in the Default Domain Policy! (There can be other GPOs at the domain level that can alter the settings in this GPO, but the thing they all do is have a Link to the Domain level!)

2. Any GPO that is linked to the Site or any OU can’t configure the account policy settings for domain users! No exceptions.
3. Any GPO that is linked to the Site or any OU does configure the local SAM for the computer that is in the path of the GPO. The rules of LSDOU still apply to the computer’s local SAM, with regard to the account policy settings. It is only the domain controllers that are exempt from this behavior. (An easy way to remember this is that DCs don’t have a local SAM, so the Site and OU GPOs wouldn’t affect them in this manner anyway.)

Account Policies at the Domain Level

The account policies in the Default Domain Policy control the passwords for all domain user accounts. This is for the single domain only! This rule is 100-percent independent of the overall Active Directory structure or any trust model that is in place. If you have an empty room domain with a complex set of password restrictions configured in the account policy, it will only affect the user accounts in the empty room domain. The GPO settings, including the account policy settings, do not inherit down to other domains in any way.

Account Policies at the OU Level

Since the account policies are already configured at the domain level, there might not be any need to configure account policies at the OU level. In most cases, you should stay away from this altogether. The reason is that the account policies configured in the Default Domain Policy meet or exceed the company’s written policy for password requirements. If a GPO that is linked to an OU is configured to modify the account policies, it could break the company’s written security policy if the settings aren’t set more secure than the GPO at the domain.

On the other hand, there are cases where you would like to have some computers adhere to a more stringent account policy than the other computers on the network. This might apply to Web servers, human resources servers, or servers that run financial applications. Remember, we are only affecting the local SAM and the user accounts that reside in the local SAM.
GPO Shortcuts

On a standard installation of Active Directory, there are many ways to access the default GPOs. The problem with all of these options is that it seems like access to the different options displays different views of the same GPOs. However, when you receive different views of the same GPO, it can cause concern as to whether they are the same thing at all.

Let's investigate the different options and methods for accessing the default GPOs. This will also help you understand how to access the other GPOs that you create in Active Directory.

ADUC

First, you can access the GPOs from inside the Active Directory Users and Computers (ADUC) console. To view the default GPOs, you'll either right-click on the domain or right-click on the Domain Controllers OU. Regardless of which GPO you're looking for, select Properties from the right-click menu. Then, select the Group Policy tab from the Properties sheet. You will see the GPO that you're looking for on this tab, as shown in Figure 18.
By selecting the GPO and clicking the Edit button, you’ll invoke the Group Policy Editor. This will show you the entire listing of the GPO.

**Default <Domain/Domain Controller> Security Policy**

Next, you can access the default GPOs from the a shortcut on the Start Menu (This must be from a domain controller.) Go to Start \ All Programs \ Administrative Tools. (Your path might vary, depending on operating system and Start Menu configurations.) From here, you can either select the Default Domain Security Policy or the Domain Controller Security Policy. When you select either one of these options, you’ll open a window that looks like Figure 19, which shows the Domain Security Policy.
Figure 19. Default Domain Security Policy is a subset of the overall Default Domain Policy.

This won’t show you the entire GPO; instead it only shows you the security policy settings. The security policy settings are a subset of the overall GPO. If you access the entire GPO (using the method described above), and expand the nodes under the Computer Configuration \ Windows Settings \ Security Settings, you’ll see there is a one-to-one relationship between this portion of the GPO and the Default <Domain/Domain Controller> Security Policy from the Start Menu.

Do keep in mind that these two views of the security settings are the same settings in the GPO. It is just a different presentation of the GPO.

Local Security Policy

The local security policy is an underused tool that is also little understood. What I’m referring to is the Local Security Policy setting that is available under the Start \ All Programs \ Administrative Tools menu option.

If you’re working on a Windows Server 2003 domain controller, you’ll find that this menu option for the Local Security Policy is missing. I’m not sure why Microsoft removed it from the menu, but my guess is that it was too confusing and caused more problems than good. However, you’ll still find the Local Security Policy on all Windows 2000 computers, Windows
When you open up the Local Security Policy on a Windows 2000 domain controller, you’ll see a subset of a standard GPO, as shown in Figure 20.

The reason that this tool is so important for the default GPOs, as well as for any GPO application, is that it shows you the local GPO and the effective GPO settings on the computer. This can be confusing, so let me explain exactly what is occurring here. The Local Setting column indicates the settings that are located in the local GPO. This may or may not be the final settings on the computer. Of course, we know there can be GPOs at the site, domain and OU location that override the local GPO settings. That is what the Effective Settings column is for. It indicates what the final settings are on the computer. This gives you a view into the settings on the computer when you open up the Local Security Policy window.

What the tool does not give you is an indication as to which GPO made the configuration and from which location, SDOU. However, there are tools that can do this, for example, the RSoP snap-in for Windows XP and Windows Server 2003, as well as the FullArmor tools. (You can download
an evaluation of Fazam tools from the FullArmor Web site at http://www2.fullarmor.com/solutions.)

Note: In my second volume in this series, Advanced Group Policy Objects, I will provide detailed information on RSoP, tools that can be used to report the RSoP and instructions for troubleshooting GPOs when the RSoP is malfunctioning.

It is clear that checking GPO application can be assisted with the use of the Local Security Policy. However, things changed radically after Windows 2000 with regard to the Local Security Policy. As I have already said before, a Windows Server 2003 domain controller no longer has the Local Security Policy as an option under the Administrative Tools.

Tip: To get the Local Security Policy on a Windows Server 2003 domain controller, you can follow the steps in the section below this one on using the Microsoft Management Console to view the default GPOs.

The other dramatic change with regard to the Local Security Policy is with a Windows Server 2003 server and a Windows XP Professional client computer. Both have the shortcut from Administrative Tools, but once you get into the interface, things have changed, as you can see in Figure 21.

Figure 21. The XP and Windows Server 2003 Local Security Policy has a different interface from the Windows 2000 Local Security Policy.
First, notice in Figure 21 that there are no longer two columns for the settings. There is only a single column, named Security Setting. This is really the same as the Effective Setting from Windows 2000. However, you can’t determine what’s a local setting or what’s a GPO setting that came from a GPO linked to SDOU. Or can you? If you look closely at the left side of the Policy column, you’ll see an icon. There are two different icons that show up. One represents the Registry. This one is the torn sheet with blue binary digits on the icon. The other represents a GPO from Active Directory. This icon is a pair of computers, with a scroll in front of them. The scroll is the standard icon for a GPO. With this information, you can decipher whether the GPO is from the local GPO or from SDOU. Those that are local have the Registry icon, and those that are from SDOU will have the Active Directory GPO icon. Tricky, but now that you know the secret, you can use the Local Security Policy again.

**Microsoft Management Console**

An almost fool proof method to view the default GPOs—or any GPO for that matter—is to use the Microsoft Management Console (MMC). The MMC allows you to open up any GPO, even the local GPO from the computer where you’re running the tool. With this method, you can open any GPO, even those that aren’t linked to a site, domain or OU.

To edit the Default Domain Policy using the MMC, follow these steps:

1. Click the **Start** button, then select **Run**.
2. Type MMC, then click the **OK** button.
3. Click **File** on the toolbar and select the **Add/Remove Snap-in** menu option.
4. Click the **Add** button.
5. Scroll down and click on the **Group Policy Object Editor** snap-in.
6. Click the Add button.

7. Click the Browse button on the Select Group Policy Object page.

8. Click the All tab.

9. Select the Default Domain Policy from the GPO list and then click the OK button.

10. Click the Finish button.

11. Click the Close button.

12. You should now see the Default Domain Policy in the Snap-ins list on the Add/Remove Snap-in page.

13. Click the OK button.

From here, you can see the entire Default Domain Policy GPO. This provides you a foolproof method to open any GPO, as long as you have the permission to edit GPOs.

As you open up the Default Domain Policy, you might notice that you can also open the Local GPO using this method too. For Windows Server 2003 domain controllers, this is a perfect way to access the local GPO, as well as see the Local Security Policy settings, which is a subset of the local GPO.
**Tip:** When you exit from the MMC window, it will prompt you as to whether or not you want to save the window. Nothing will be deleted from the GPO if you don’t save the window. This is only if you want to save the snap-in list for easy access. Most of my Windows Server 2003 domain controllers have a saved MMC for the local GPO, which I save to the Administrative Tools list.

**Gpedit.msc**

To directly access the local GPO, you can run the GPEDIT.MSC command from the Start | Run option or a command line. This provides the same result as using the MMC to open the local GPO for the computer where you run the command. You can only open the local GPO using this method though, which makes it rather limiting. The great thing about this option is that it is fast—much faster than attempting to open the MMC and add a snap-in.
Group Policy User and Computer Configurations

In this section I discuss the two major areas of a GPO. We already know that GPOs apply to either user accounts or computer accounts. Here, we’ll break down each of these sections that is located under a default GPO so you fully understand what each section can do for you. We won’t be diving into each individual GPO setting, since that is already done for you at the following locations.

- Windows Server 2003 Help and Support Center (search on “Group Policy”).

With almost a thousand settings in a Windows Server 2003/XP GPO, you can’t expect to memorize them. Rather, it is more important to understand the logical structure and areas of the GPO. With this knowledge, you can find the GPO that you’re looking for, or you can search the documents provided to find the GPO setting.

Computer Configuration

The top half of every GPO is dedicated to configuring the computer accounts. As you may have noticed in many of the figures in this book, you can see the Computer Configuration section of the GPO during editing. There are many sections in the Computer Configuration section of the GPO, each having a distinct area and function. We’ll look at each section, discuss how to configure difficult settings, cover the key configurations for
areas that have many policies, and explore what the area is designed to modify for the computer accounts.

**Software Settings**

This is designed to install software to the computer account. The reason that many administrators like to install to the computer account is that every user that logs onto the computer will have the software. Also, a benefit to installing to the computer is that the software is installed when the computer is restarting. Basically this provides for immediate access to the application when every user logs on.

Software for computer accounts can only be Assigned (we’ll see that for user accounts they can be assigned or published). An assigned application will install the application and place a shortcut to the application on the Start Menu automatically. Software that is assigned uses Microsoft Installation Packages, or MSIs. Many applications now provide MSI versions for installation. Examples include: Administrative Tools, Microsoft Office and Service Packs.

To prepare a GPO to install software, follow these steps:

1. Expand the **Software Settings** node located under the Computer Configuration section of the GPO in the Group Policy Editor.

2. Right-click on the Software installation node and select **New Package**.

3. Browse for and select the MSI package that you want to deploy.

4. Then select the **Open** button. Note: If you have used a local path, instead of a network path, to the MSI package, you’ll receive the error message shown in Figure 22, below. This indicates that the software package will fail to apply to computer accounts, since the path to the MSI package isn’t available to network computers.
Figure 22. You must use a network path, not a local path, when configuring the location of the MSI package in a GPO.

5. Click the Assigned radio button, then select OK.

6. The new software deployment package will show up in the list of software to be installed.

7. Close the GPO editor and the application is ready to be installed.

You could have selected “Advanced” (“Advanced Published or Assigned” for Windows 2000) during Step 5. If you had chosen this radio button, you would have been able to customize the deployment package. You could have controlled software upgrade scenarios, modifications to the MSI package and deployment control.

Windows Settings

Windows settings for computer accounts have three major subcategories. Two subcategories have extensive policies and categories to choose from. By far this is the most useful area in the GPO under the Computer Configuration section. Here you can configure almost any security setting related to the computer account. If you’re missing a setting that isn’t there by default, you can customize almost any setting using custom security templates.
Scripts (Startup/Shutdown)

The first subcategory under the Windows Settings involves the scripts that can be targeted to computer accounts. This is a new feature for Active Directory that can be quite powerful. There are two different settings for computer-based scripts: startup and shutdown. Each is straightforward, yet provides flexibility and power.

Startup scripts can map drives, connect to printers, start services, stop services and much more. The great thing about startup scripts is that they will configure the computer before the user attempts to log on. You can use scripts that include the following file types: BAT, EXE, and VBS. This array of script types give you the freedom to do almost anything that you want in the script.

Scripts run as the Local System. This gives them full capabilities that are associated with being able to run as the Local System.

Shutdown scripts can clean up network connections, stop services, back up files and more. A shutdown script can speed up shutdown of a computer, since it will clean up services that can take a long time to “time out” during the shutdown process.

Adding a script is as simple as right-clicking on either Startup or Shutdown and selecting Properties from the menu. Then, just select the Add button to select a script that you want to use. Ideally, the scripts will all live under the NetLogon share, but you can browse for the script anywhere on the computer.
Security Settings

One of the most exciting areas in all of the GPOs categories is the Security Settings for the computer accounts. This is where many quality security settings are configured. Plan to spend a lot of time going over these settings, to ensure that you haven’t missed any and to determine which ones should apply to each type of computer account in your organization.

Account Policies

One of the most important configurations in any GPO involves Account Policies. This configures the rules for passwords on the domain controllers, for domain user accounts, and for all members of the domain. The account policies are broken down into three different areas of configuration: Password, Account Lockout, and Kerberos. These configurations, along with their default settings are described in the “Account Policies Break The Rule” section of this book.

Local Policies

The “Local Policies” is an unfortunate name for this category of GPO settings. The reason it is unfortunate is that the word “Local” is hard to scope when you’re working in a GPO. Here “Local” is referring to the local computer that it will affect. The settings on the local computer that this section affects include:

- Audit Policies. The audit policies control what will be audited and recorded in the security log of the Event Viewer. When these policies are configured, they will modify the settings on the target computer.

- User Rights Assignment. User rights are extremely important for security control. When these policies are configured, they modify the target computer, controlling who can do what on that computer. Examples of important user rights include: Logon locally; Access this computer from the network; and Backup and Restore folders and files.
• **Security Options.** Here is where much of your time will be spent configuring GPOs. The list of security options provides you with a fantastic set of options to control almost any aspect of security on the target computer. For a detailed explanation of what each GPO policy does, refer to the policysettings.xls link listed earlier on Microsoft’s Web site. Also, the following list of policies should be researched and tested for your environment, since they provide excellent security for most companies:

  o Accounts: <All configurations under this category>.
  o Interactive logon: Do not display last user name.
  o Interactive logon: Do not require Ctrl+Alt+Delete.
  o Interactive logon: Message text for users attempting to log on.
  o Interactive logon: Message title for users attempting to log on.
  o Microsoft network client: <Digitally signed communication>.
  o Microsoft network server: <Digitally signed communication>.
  o Network access: <All configurations under this category>.
  o Network security: <All configurations under this category>.

*Note: This isn’t an exhaustive list of the policies under the Security Options section. The other policies are extremely important too, but this list includes the most common policies a company would want to implement. Be sure to research and test all policies to see if your environment will benefit from their configurations.*
Event Log

This set of policies allows you to control almost any aspect of the event logs that exist on the target computer. It is always suggested that you make your event logs large enough to track all events between backups of the archived logs. You can also control how the logs are cycled using these policies. The following is a list of the control aspects of the application, security and system logs.

- Log file size.
- Guest group access to the log file.
- Length of time to retain the log file.
- Retention method for the logs.

Restricted Groups

This is one of the most powerful yet confusing areas of the Computer Configuration policy options. The restricted groups allow you to control the membership of groups on the target computer. You can control which objects have membership in certain groups, as well as which groups the group is a member of, as shown in Figure 23, below.
Figure 23. Restricted Groups allow you to control the membership of the group, as well as which groups the group has membership in.

This policy can be useful for controlling both members of the domain, as well as groups in Active Directory. You should control the following groups in the local SAM of computers in the domain:

- Administrators (typically want to ensure Domain Admins is a member).
- Power Users.
- Backup Operators.
- Remote Desktop Users.

For many of these groups, you’ll need to type the group manually into the text box after you select the Add button. The reason for this is that the GPO editor takes the list of users and groups relative to the computer that
you’re administering the GPO from. If you’re administering the GPO from a domain controller, you won’t be able to access the list of groups from the local SAM on the target computer you want to control with the policy.

**System Services**

If you haven’t taken advantage of controlling services through GPOs yet, you’ll want to check out this section of the policies. You’re able to control any service running on any computer from these policies. You have the option to control how the service starts, as well as the ACL for the service, as shown in Figure 24, below.

![Security Policy Setting](image)

*Figure 24. GPOs can control system services at boot time, as well as the access to the service controls.*

There are two key functions of the system services in a GPO. First, you can control how the service starts. You can disable the service, such that the service can’t be started without first enabling the service. Automatic will start the service when the computer starts. Manual won’t start the service, but allows for the service to just be started by an administrator or an application that requires the service.
The control of starting, stopping, pausing, etc. services can also be controlled using GPOs. Services have an ACL, which is only accessible through scripting or the GPO. You can’t see the ACL on the service from the Services module or the Computer Management console. The power and control over the services using this security is useful, to control who can control the services on the target computer.

The only essential configuration that can’t be accomplished from the GPO is establishing the service account. This must be done at the service on the local computer.

**Registry**

The ACLs for Registry Keys can be controlled by this portion of the GPO. This can be limiting, since it is only the Registry Key, but the main access to values and data in the Registry is controlled at the key level. After the ACL is configured for the key, the ACL inheritance can also be controlled, as shown in Figure 25, below.

![Template Security Policy Setting](image)

*Figure 25. The Registry Key ACL inheritance can be controlled from the GPO.*
These settings allow you to control how the ACLs on the objects below this key are controlled, as well as how the ACLs on this key are controlled. The top portion of Figure 25 relates to the subkeys and the bottom portion relates to the permissions on this key.

File System

The file system is similar to the Registry, in that you can control both the ACL and the inheritance of the ACLs on the folder as well as subfolders. You can control both files and subfolders using this GPO policy.

If the folder path or file doesn’t exist on the computer where you’re administering the GPO from, you can just manually type in the path for the folder or file. The path needs to be exact and it needs to exist. If the policy is incorrect or attempts to configure a non-existent file/folder, the other policies will most likely fail because this policy failed.

Wireless Network (IEEE 802.11) Policies

This is new for Windows Server 2003 and Windows XP Professional GPOs. There are no wireless network policies configured by default, but the wizard will walk you through the creation of a new one. Once you have the new policy name established, you can configure the following key areas of a wireless connection.

- **Networks to access.** This controls which network the target computer will access. The list includes any available network access point, infrastructure networks only, or ad hoc networks.

- **Preferred networks.** This option in the policy allows you to configure one or more preferred networks. The SSID is required, as well as the configuration for the wireless network key (WEP). There is an entire tab related to the IEEE 802.1X authentication. This allows you to specify how credentials, such as smart cards or other certificates, are used for authentication.
Public Key Policies

This isn’t a new section to the Windows Server 2003/XP GPO, but some of the settings are new. If you’re using certificates for authentication, e-mail or any other secure communication, you’ll want to take advantage of the new certificate control policies. The following is a list of the different areas under this policy.

- *Encrypting File System.* This policy controls which user accounts will function as a Data Recovery Agent (DRA) for when encrypted files need to be salvaged. It also allows a configuration that establishes that a DRA isn’t needed to encrypt files.

- *Automatic certificate request.* This allows an administrator to control which types of certificates can be automatically requested by a computer.

- *Trusted Root Certification Authorities.* This allows an administrator to control the certificates, certificate trust list and certificate revocation list in the target computers certificate store. This is useful if your organization has its own root CAs that aren’t installed on servers. This policy allows you to distribute the root certificates.

- *Enterprise Trust.* This allows an administrator to control trust to external CAs.

Software Restriction Policies

These policies are new for Windows Server 2003 and Windows XP Professional. When you use software restriction policies, you can define a default security level of Unrestricted or Disallowed for a Group Policy Object (GPO) so that software is either allowed or not allowed to run by default. Exceptions can be created to this default security level for specific software. You can create the following types of rules:
• Hash rules

• Certificate rules

• Path rules

• Internet zone rules

The following tasks can be performed by using these policies:

• You can control which software can run on a computer.

• You can permit specific software to run on multiple-user computers.

• You can control trusted publishers to your computer.

• You can prevent software from running on any computer that is in the domain.

The path rule is popular, since it can control an entire path on the target computer. A common path rule will be a combination of multiple rules. One rule will lock down the computer from running any applications. Then, additional specific paths will be established to just allow certain applications.

Here’s a sample policy that uses the Path Rule method. This policy controls the WordPad program on the computer. It only allows Wordpad.exe to run on the computer, and nothing else.

1. The security needs to be set to Disallowed and the default path rule that allows all applications to run is removed. This will remove the ability for all applications to run.

2. Then an individual rule needs to be created for Wordpad.exe.
3. Finally, the additional path rule that you have created needs to include the path for Wordpad.exe, which will exempt it from the removal of the default path rule deletion.

The hash rule is also common. It is common because a sharp user will change the name of files to get around some policies. Not so with the hash rule. The hash rule uses the signature inside the application to lock down allowed or denied access to the application.

Here’s a sample policy that uses the Hash Rule method. This policy disables Solitaire and won’t let it run, even if the name of the original sol.exe is changed.

1. Create a new hash rule.

2. Then, the new hash rule needs to point to sol.exe.

3. Finally, you configure the hash rule to use the hash signature, instead of just the name.

**IP Security Policies on Active Directory**

These policies are powerful, as well as complex. The IP Security policies can control how computers communicate with one another on the network. The main goal of IP Security is establishing how the computers will protect the data as it is sent from point to point. There are three default IP Security policies, each one having an established configuration for the encryption, authentication, and ports that can be used during communication. The three default policies include:

- **Client (Respond only).** When this policy is configured, it allows the computer to use IP Security configurations contained within it when it is asked to use IP Security from the computer initiating the communication.
• **Secure Server (Require Security).** When this policy is configured, it forces the computer to use IP Security for all communications. If the computer that this computer initiates the communication with couldn’t use IP Security, the connection would fail.

• **Server (Request Security).** When this policy is configured, it attempts to use IP Security with all communications to other computers. If the computer that this computer initiates the communication with couldn’t use IP Security, it would just communicate without any encryption or secure communications.

All of these policies can be configured for both a client computer and server computer. The phrasing of Client and Server in the policy only specifies which computer is performing the initial communication and which is receiving the initial communication.

For more information on IP Security, go to http://www.microsoft.com/technet/prodtechnol/windows2000serv/evaluate/featfunc/ipsecure.mspx to read a Microsoft white paper.

### Administrative Templates

The administrative templates are packed with excellent configurations for a wide variety of areas of the computer. All of the administrative templates configure a portion of the Registry. When configuring administrative templates, be sure to pay attention to the following concepts.

• Enabling a policy enforces the action that the policy specifies.  
  *Example:* If the “Don’t display welcome screen at logon” policy is enabled, the Welcome screen won’t be displayed anymore.

• Disabling the policy will do the opposite of what the policy specifies.  
  *Example:* If the “Don’t display welcome screen at logon” policy is disabled, the Welcome screen will be displayed at logon.
• Setting a policy to Not configured will neutralize this GPO’s ability to modify the Registry value. The only way that the Registry value will be altered is for a different GPO (local, or from SDOU) to configure this policy.

• Setting a policy from enabled to Not configured or disabled won’t set the default value of the Registry back. The GPO or computer doesn’t keep track of old values. For a policy that is either on or off, the behavior will function like a light switch. However, when there is a configuration involved, such as a DNS suffix, this value will be recorded in the Registry. When the policy is no longer affecting the computer, the values won’t go back to an original state; it will just remove the policy settings from the existing GPO.

• Watch closely for double negatives in the policy wording. Sometimes enabling a policy will remove a setting or feature, where other times it will add a setting or feature.

  Example: The “Disable legacy run list” will need to be enabled for the run list to not be functional. If this were disabled, it would disable a “Disable,” which would effectively enable the setting.

Windows Components

The Windows components consist of specialized areas of the computer that can be controlled. The areas that can be controlled under this section include:

• NetMeeting

• Internet Explorer

• Application compatibility

• Internet Information Services
• Task Scheduler

• Terminal Services

• Windows Installer

• Windows Messenger

• Windows Media Digital Rights Management

• Windows Media Player

• Windows Update

Most of these categories are new for Windows Server 2003 and XP, mainly because of the influx of requests to get them in the interface. Since the request for these settings was so high, they are all popular. Many settings are basic in that they just disable the service completely. Other settings control finite aspects of the applications, such as the Internet Explorer and Terminal Services categories.

**System**

Another section that has blossomed from Windows 2000 to Windows Server 2003 and XP is the System section. Here you have a full array of policies categories and settings ranging from User profiles down to Windows Time Service. Some of the other key categories under the system section include:

• User Profiles

• Logon

• Disk Quotas

• Group Policy
- Remote Assistance

- System Restore

One group of policies that need mentioning here is under Group Policy. There are 10 policy settings that are essential for a secure GPO environment. These include:

- Registry policy processing
- Internet Explorer Maintenance policy processing
- Software Installation policy processing
- Folder Redirection policy processing
- Scripts policy processing
- Security policy processing
- IP Security policy processing
- Wireless policy processing
- EFS recovery policy processing
- Disk Quota policy processing

All of the policy settings have a key configuration associated with them. If you open up any of these policies, you’ll see an interface that is similar to Figure 26.
Figure 26. An entire group of policies can apply policies to computers, even if the GPO hasn’t changed, allowing for a more secure environment.

You will notice that there’s a check box associated with the “Process even if the Group Policy objects have not changed.” This applies the GPO to the target computer even if there haven’t been any alterations to the GPO. The reason this is such a great setting is that if the local administrator of the target computer changes a Registry value or other system parameter that was set by the GPO, at the next refresh it will be set back to what the GPO indicates.

Network

The network section of the GPO allows the administrator to control key elements of the networking capabilities of the target computer. The three most common areas that are used under the network section include:
• **DNS Client.** This controls the DNS configuration of the target computer. This isn’t limited to the DNS suffixes, but also how the target computer updates DNS automatically.

• **Offline Files.** This policy controls almost every aspect of offline files on the target computer, from denying offline files to controlling the balloons that are used by offline files.

• **Network Connections.** Although the list of policies is short, the settings are common. This area allows you to control both Internet Connection Sharing and Internet Connection Firewall on the target computer.

**Printers**

The policies in this section control how printers are published to Active Directory, as well as how the client computers that are targeted by this GPO locate the printers in Active Directory. An important theme in these GPOs is the “Printer Location” capabilities in Active Directory. This allows a user to search more efficiently for the printers, not only within the directory, but physically in the building where the user is located.

**User Configuration**

**Software Settings**

This is designed to install software to user accounts. The reason that many administrators like to install to the user account is that the software will follow the user, if the user moves from computer to computer. For security and licensing reasons, even if a targeted user uses an application on a computer, does not mean that a non-targeted user can use the application that is available on that computer.

For example, if Joe logs onto a computer named XP1, Joe will be able to use all software that is targeted to his user account. Assume that Joe has Microsoft Word assigned to his user account. When Joe logs on, he will
have Word on the Start Menu. When Joe logs off of XP1, Word will still be installed. However, when Sally, who does not have the GPO applying to her account, logs onto XP1, she won’t have access to Microsoft Word. This access even goes as far as the local Administrator. If the local Administrator logs onto XP1 and goes to the folder where winword.exe resides, the Administrator will even get an access denied for running the application.

Software for user accounts can be Assigned or Published.

- **Assigned.** This puts the application on the Start Menu, as if the application were installed. The application is installed when the user tries to open up the application or attempts to open a document that is associated with the application.

- **Published.** This puts the application in the Add or Remove Programs list. The user can either install the application from the Add or Remove Programs list, or he or she can simply attempt to open a document that only the application can open. In either case, the application will install on the computer that the user is using.

Both options provide access to the application on-demand, either by accessing the application or a document that requires the application to be installed.

**Windows Settings**

**Remote Installation Services**

Remote Installation Services (RIS) allows an administrator to deploy the operating system from a boot time environment. The user is able to select an “image” from a list of possible computer operating systems and configurations. These policies allow the administrator to control some of the extras that are associated with RIS. These extras include custom setup options, automatic restart options and an additional set of tools to be used with the installation.
Scripts (Logon/Logoff)

There are two settings for user based scripts: logon and logoff. Logon scripts can map drives, connect to printers, start services, stop services and much more. You can use scripts that include the following file types: BAT, EXE and VBS. This array of script types give you the freedom to do almost anything you want in the script. Logoff scripts can clean up network connections, stop services, back up files and the like.

Security Settings

The security settings for the user configuration aren’t nearly as glamorous and robust as for the computer configuration. For user accounts, there are only two categories of configurations: Public Key Policies and Software Restrictions.

Public Key Policies

For the user accounts, it is only possible to control the Enterprise Trust, which mainly controls the trust to external CAs.

Software Restriction Policies

The software restriction policies for the user account are identical to those of a computer account, except that they will target only the one user that is logged onto a computer, not every user that logs onto the computer. This is advantageous if the restrictions for users vary between different types of users. This allows for multiple users to access the same computer, but have access to different applications.

For more details on the different rule options and capabilities of software restriction policies, see the section, “Software Restriction Policies.”

Folder Redirection

One of the most used policies in all of the policy options are the folder redirection policies. These policies allow administrators to control where
user information is stored, for security, compatibility and consistency.

There are four main areas that can have redirected folders, which include:

- **Application Data.** This folder is located in the user’s profile. This is one of the key folders for the applications and their configurations for each user. Therefore, it’s important to have this folder redirected to a network folder, so it can be secured and backed up regularly.

- **Desktop.** In order to provide a consistent look and feel for every user in the company or a subset of users in the company, you can have users access a centrally located folder that configures their desktop.

- **My Documents.** By default most applications store files on the local computer, under the My Documents folder. This is great for home users, but for companies it is a security and stability issue to allow users to store files locally. This will redirect the My Documents and My Pictures folders to a network drive for control and backup reasons.

- **Start Menu.** Like the Desktop, it is nice to deliver a consistent Start Menu to every user in an area. This provides for easier training, support and troubleshooting.

Each setting comes with some unique options for configuration. First, each folder has the ability to control all users or just a subset of users who have membership in a group. Then, you can control what privilege the user will have over the redirected folder. Finally, there are options to control how the data is moved back and forth between the local computer and the central shared drive, when the policy is implemented and removed, as shown in Figure 27, below.
Folder redirection allows control over the content when the policy is implemented and then removed.

Internet Explorer Maintenance

The user targeted IE Maintenance is a little different than the computer targeted IE policies. These policies address the individual choices that users make most often within IE. The categories that can be controlled using this policy section include:

- **Browser User Interface.** This set of policies can control the look and feel of the IE interface. Areas of control include the title, logos and toolbars.

- **Connection.** This set of policies controls how the IE browser gains access to the Internet. This could be via modem, LAN, etc.
This set also configures the Proxy settings, similar to what the computer configuration provided. *Note: If there were a setting that both the user and computer configuration established, the computer configuration setting would take precedence.)*

- **URLs.** This allows control over the favorite URLs and the important URLs.

- **Security.** This set of policies allows control over the security zones and content ratings, as well as over Authenticode settings.

- **Programs.** This allows control over the different IE-based applications and programs. This includes the HTML editor, e-mail, newsgroups, Internet calling, Calendar and contact list.

**Administrative Templates**

These templates provide the same characteristics as the computer-based template settings, except that these policies will modify the HKEY_Current_User Registry hive, where the computer settings modify the HKEY_Local_Machine hive.

**Windows Components**

The Windows components consist of specialized areas of the computer that can be controlled. The areas that can be controlled under this section include:

- NetMeeting
- Internet Explorer
- Application compatibility
- Help and Support Center
• Windows Explorer

• Microsoft Management Console

• Task Scheduler

• Terminal Services

• Windows Installer

• Windows Messenger

• Windows Update

• Windows Media Player

Most of these categories are new for Windows Server 2003 and XP, and match the computer categories almost exactly. There are different settings comparing the computer and user policies. Many of these settings are essential in a company domain, due to the security and excess functionality that these tools give the typical employee.

Start Menu and Taskbar

This set of policies controls almost every aspect of the Start Menu and Taskbar. There is almost nothing that you can set to control these areas of the user environment. If you aren’t careful, you can remove almost every option from the user’s Start Menu, allowing them only a few options for getting work done. Many companies have taken this approach, not allowing any extra applications on the computer to restrict the user’s capability for browsing the Internet or wasting time with “Spider Solitaire.”
Desktop

This set of policies controls the Active Desktop environment as the desktop icons. The control goes from the icons, to the icon context menus, and the ability for a user to save settings upon exit related to their desktop. This set of policies also controls the user’s Active Directory search options. This is a bit strange to tuck these settings here, but if you need to alter how the user searches Active Directory, you’ll need to look here for those settings.

Control Panel

The Control Panel is full of applets that control important aspects of the computer. Many administrators use these policies to restrict the access to these areas, including:

- *Add or Remove Programs.* If the user can’t add or remove programs, the computer will remain more secure and stable. This set of policies includes an option to completely remove the applet from the user’s Control Panel.

- *Display.* It’s easy for a user to incorrectly set a screen resolution or refresh rate that isn’t compatible with his or her video adapter or screen. These options can be taken away with policies in this section.

- *Printers.* These policies control how users use and access printers on the network.

- *Access to specific control panel applets.* This policy allows you to specify which applets a user can access and which ones the user can’t access.

Shared Folders

This is a small but important section for control and security. The two policies in this section control whether or not shares can be published to
Active Directory and whether or not DFS (Distributed File System) roots can be published to Active Directory.

**Network**

Like the computer configuration, this section provides control over the network connections on the computer. This just controls whether or not the user can control the settings. There are two categories under the network section: offline files and network connections. It’s common to configure the network connections policies, to ensure that users can’t redirect their network settings to locations that will allow them to access either private data, or data that they shouldn’t be working on during business hours.

**System**

These policies allow control over many different areas of the user environment. Many are common to a corporate setting, to ensure that users are working in a secure and stable environment. Some of the key categories under the system section include:

- **User Profiles.** These policies allow the administrator to control the profile size, as well as what information is stored in the roaming profile.

- **Ctrl+Alt+Del Options.** These policies configure the options that are available to the user during the logon process, and when he or she selects a warm reboot during a session.

- **Logon.** An important set of policies, allowing the administrator to control the run once list and the legacy run list for the user’s environment.

- **Group Policy.** A variety of settings related to GPOs for the user. Key policies control slow link detection, refresh interval for the user portion of the GPO and specify how the user interfaces with the administration of GPOs.
The Final Word

Group Policy Objects have many caveats associated with them. There can be multiple GPOs, GPOs at the LSDOU, blocked GPOs, no override GPOs, filtered GPOs, WMI filters attached to the GPOs and others. However, if you can get by without most of these complex settings, GPOs can be implemented quickly and efficiently. A simple implementation of GPOs also provides for a more stable environment that's easier to troubleshoot. Regardless of where you head with your GPO design, make sure you consider the GPOs when you design your OUs. You will thank the time you invested reading this report in the end.

Be sure to watch for the next two reports in this GPO series -- Advanced GPOs and Troubleshooting GPOs -- on MCPMag.com.