Group Policy Basics - Part 2: Understanding Which GPOs to Apply

srachui
15 Feb 2012 3:09 PM

- 42

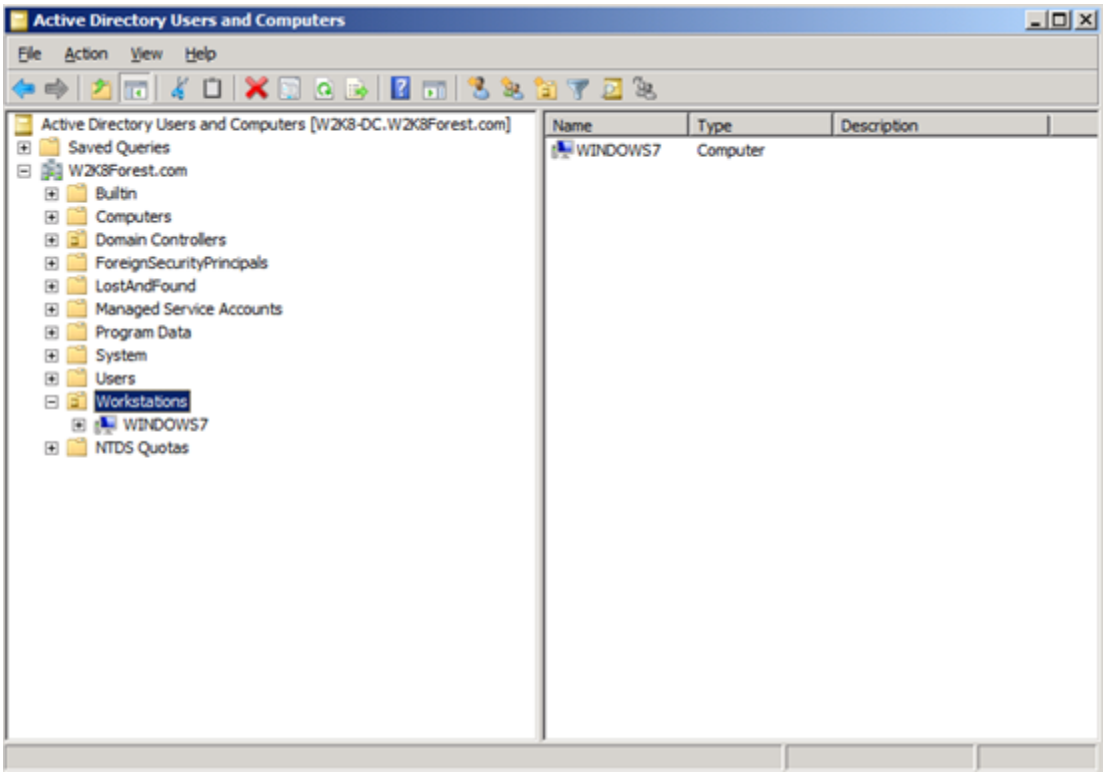
In the previous post, I talked about the structure of a GPO. Now, I'll turn to the question of what a client does in order to apply the settings that we've configured in our GPOs. The processing of GPOs is initiated from the client side rather than being pushed from your Domain Controllers. As such, your client have to understand several things to process the correct GPOs in the correct way. In order to properly understand this, we need to look at a few additional concepts.

How Does a Client Know Which GPOs to Apply?

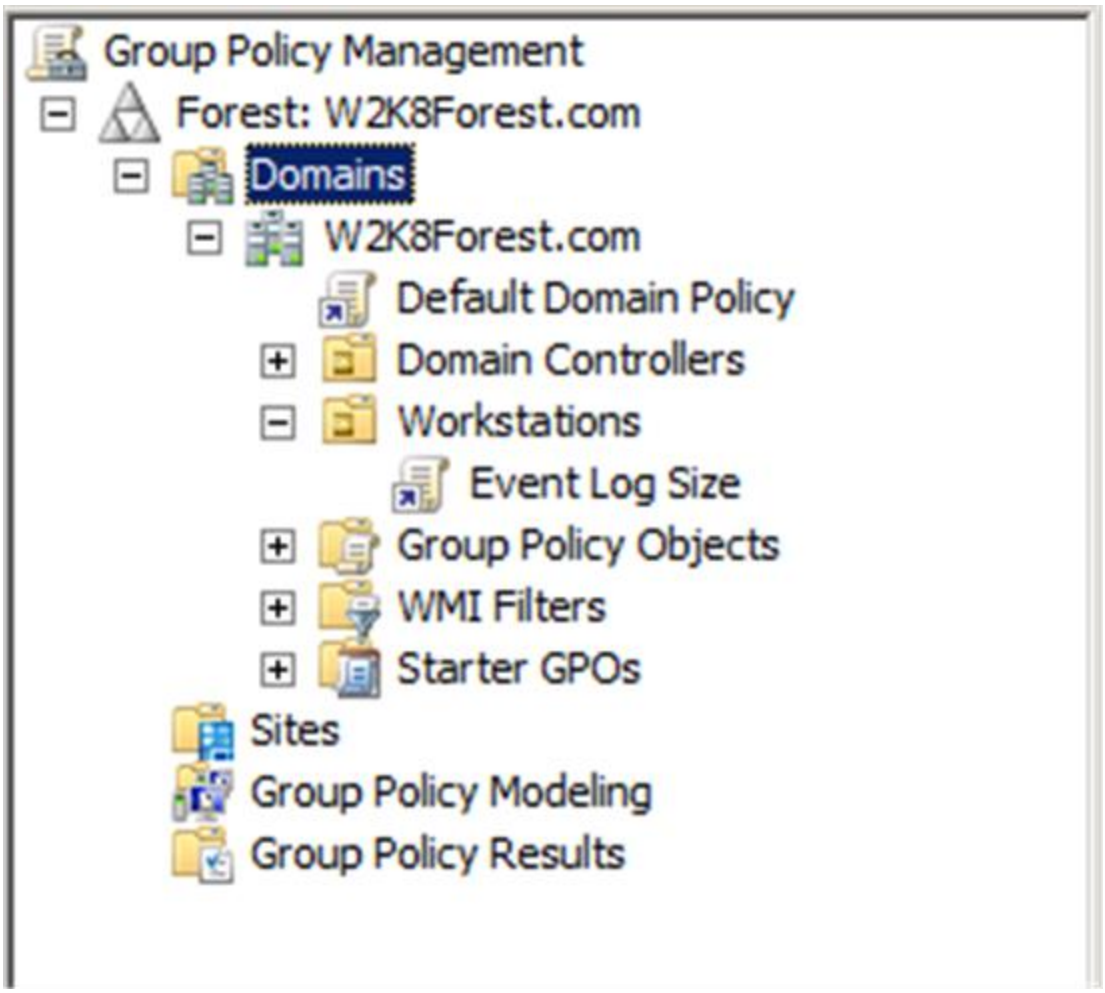
There are two types of GPOs. There are GPOs that are configured locally on the client machine and are always processed, and there are GPOs linked within the Active Directory structure itself. While the client knows that is needs to process its local GPO, it's not as clear which GPOs in the directory structure apply to it. Within the directory, GPOs can be linked to the following levels:

- Site
- Domain
- Organizational Unit

Depending on where the client object is located determines which GPOs it applies. For example, consider the following scenario:



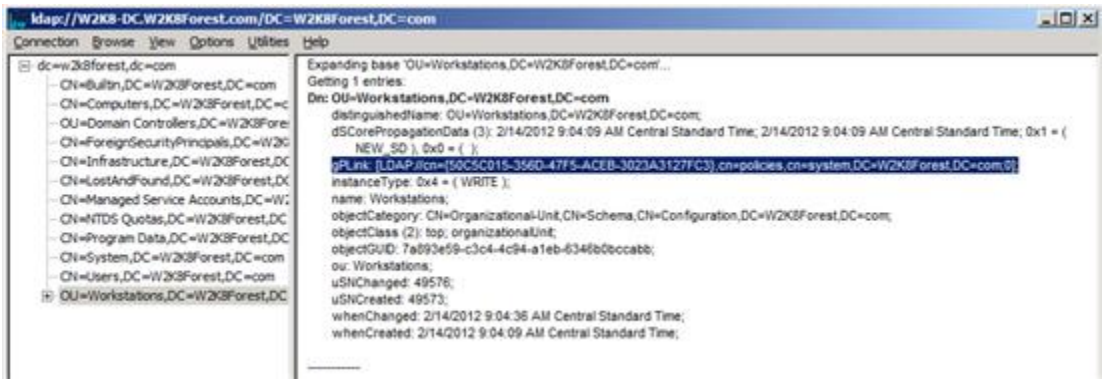
Here we see that the workstation named *Windows 7* is within the Workstations OU that is part of the W2K8Forest.com domain. Though we don't see it on this screenshot, the *Windows 7* client also belongs to the Active Directory site known as 'Default-First-Site-Name'. Given this, which GPOs need to be considered by our client machine? We already know that any local settings on the client itself will need to be processed. And if we look at the GPMC, we can see that two additional GPOs exist that the client must consider:



These two GPOs are the *Default Domain Policy* linked at the domain level and the *Event Log Size* linked to the Workstations OU. We can also see that there are no GPOs linked to any sites. So we know that our possible list of GPOs includes:

- Local GPO
- Default Domain Policy
- Event Log Size

The way the client actually sees these is a bit different. In order for your workstation or server to determine whether it needs to process any policies, it looks for the gPLink attribute that exists within certain Active Directory objects. This attribute, when populated, points to the name and location of the GPO that the client must consider. Take a look at an example of this below:



Using the LDP tool, we can see that the gPLink attribute is populated for the Workstations OU. Looking at it closely, we can also see that it is pointing the client to the Group Policy Container for a specific GPO (which we already know is the Event Log Size GPO). In the previous post, we've already seen how the GPC function so I won't cover that again. Here it's just enough to know that this is how the client learns which GPO it needs to look up.

Sticking with our scenario, we learn that gPLink is also populated on our domain object, but that it isn't populated on the site where our client belongs. So we end up with the list of GPOs already enumerated above. Now what do we do with them?

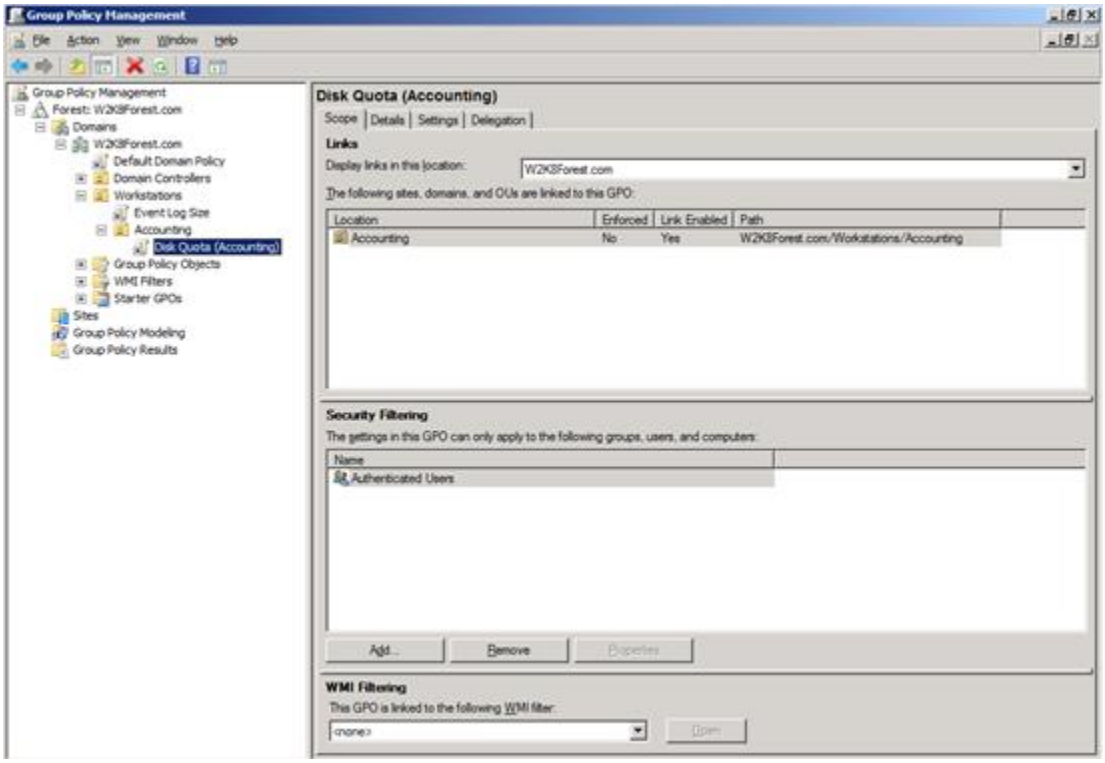
Processing GPOs: Precedence

Because it's possible (and even likely) that you may have multiple GPOs to apply, there is always the possibility that these GPOs will have conflicting settings. In this case, how do we know which GPO will win and have its settings applied? The simple rule to remember is that the last GPO applied will overwrite any settings applied earlier. And the GPOs closest to the client location in the directory structure will be applied last. The order goes as follows:

- Local
- Site
- Domain
- Organizational Unit

What this means is that if you've set something on your Local GPO but your domain administrators require a different setting, your local setting will be overwritten. The same thing applies to situations where the domain may have a default policy but your busines unit may have more specific needs. In this case, a default setting can be configured and your business unit can override this setting to apply the one your group requires.

In our example above, suppose that the Default Domain Policy GPO set a disk quote for the domain at 50 MB. However, your business unit requires that your workstations have 100 MB quotas. Your administrators could set a policy at the OU level to allow these settings for your group. Your directory structure might look like this:

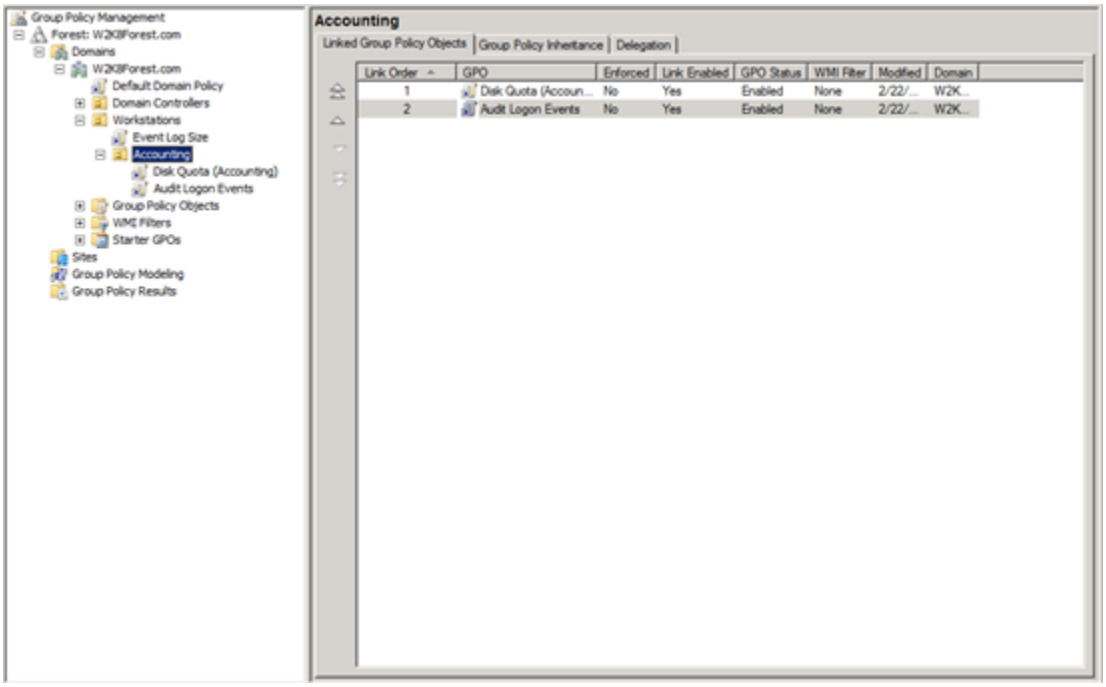


Note here that we have a new OU within the Workstations OU that we've named Accounting. We have also created a new GPO called *Disk Quota (Accounting)* that we've linked to the Accounting OU. Now, objects within the Accounting OU will have the following GPOs to apply:

- Local GPO
- Default Domain Policy
- Event Log Size
- Disk Quota (Accounting)

In this case, if the *Default Domain Policy* assigns a value of 50 MB as the default disk quota for the domain, the *Disk Quota (Accounting)* policy will overwrite it because it's applied last.

One final point about precedence and which GPO will apply in what order. What if you have configured two GPOs at the same OU level? How do we know which GPO will apply first and which one will win if they have competing settings? In this case, you must rely on the GPMC to tell you this. You can also configure the order in which these GPOs will be processed as needed. The following screenshot shows two GPOs that will be applied at the Accounting OU level:

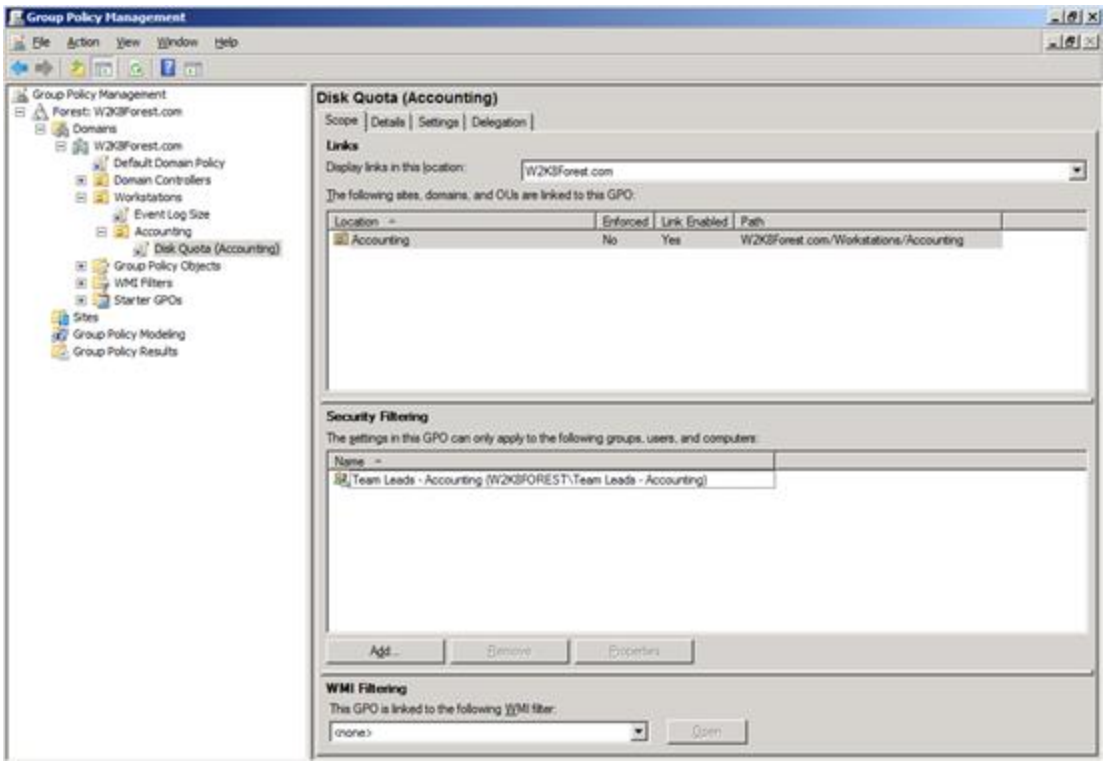


From looking at the screen, you can see that these two GPOs are numbered. The way in which GPOs are applied is from the highest number to the lowest number. So in this case, the *Audit Logon Events* GPO will apply before the *Disk Quote (Accounting)* GPO. If you want to alter this order, all you need to do is select the GPO you want to move and use the arrows on the left-hand side of the screen to move it up or down in the list.

Filtering a GPO

Before we go any further, we need to look at two more concepts that will determine whether GPO settings are applied to your client. The first is GPO Filtering. This feature allows further granularity in the way that GPOs are applied in your environment. Even when a GPO is linked within a part of your directory (say, an OU) you may not want that GPO to apply to every object within that container. You can control this by assigning permissions for who can process your GPO. This is known as filtering.

When you filter a GPO, you specifically designate which users, group and computers are allowed to apply a GPO. For example, you may only want the team leads within the Accounting group to get 100 MB of disk space for their disk quota, so you decide to configure a group called *Team Leads - Accounting* and filter the GPO on that group. If you did this, it would look like the following:



You'll notice that in the Security Filtering pane we now have only the *Team Leads-Accounting* group. This means that even if an object is within the Accounting OU, it will not apply the *Disk Quota (Accounting)* settings unless it belongs to the *Team Leads - Accounting* group.

NOTE: It is easy to allow your GPOs to become VERY complicated very quickly through the use of security filtering. Use of security filters should be carefully planned beforehand (as should everything with your Group Policy infrastructure).

Security Filtering Under the Hood

Though we can certainly add and remove users, computers and groups from the securtiy filtering window in the GPMC, it's also helpful to know what's actually happening under the hood when we do this.

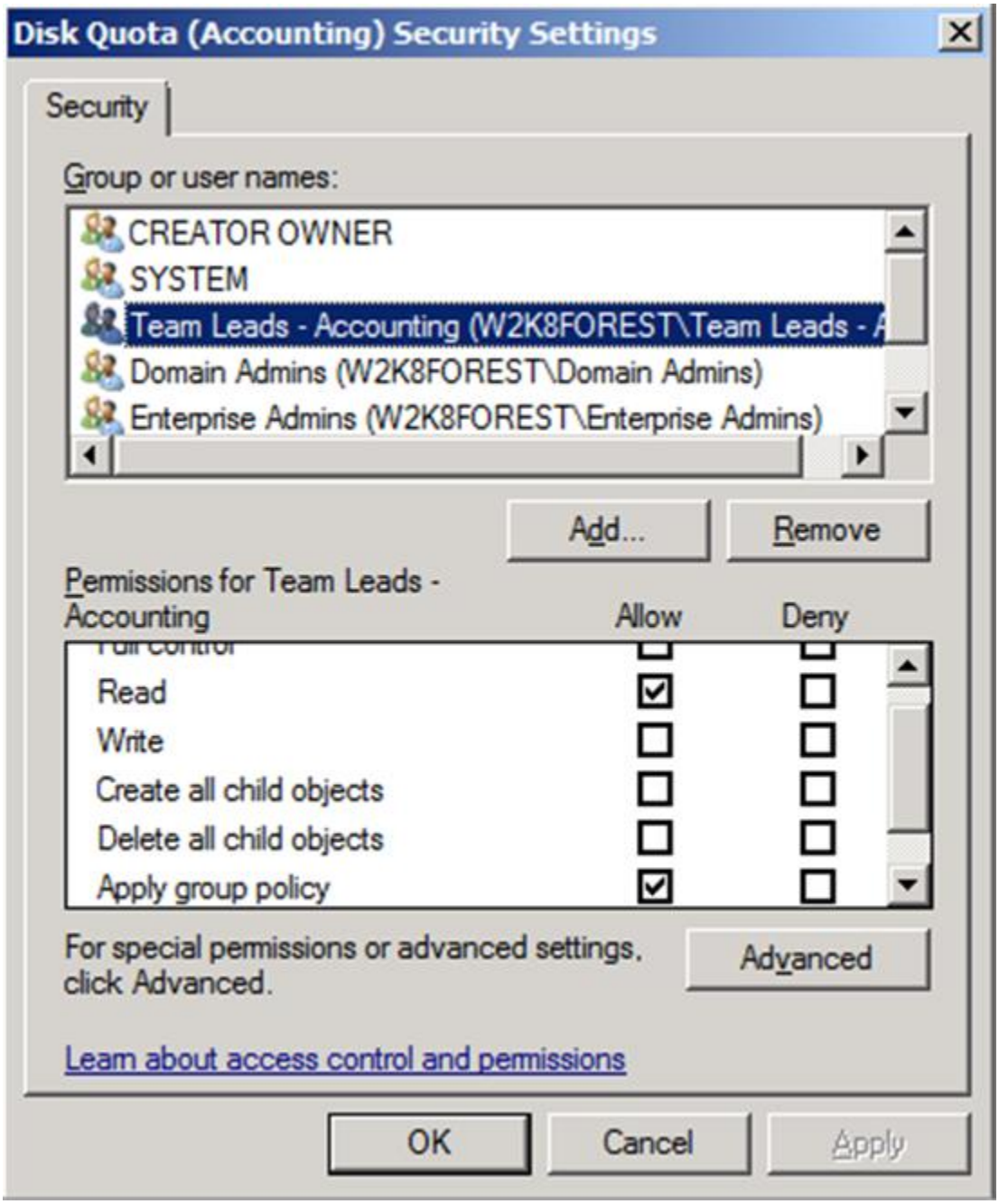
In order for a GPO to apply to an object, that object must have two rights over that GPO. These are:

- Read
- Apply Group Policy

When a user, computer or group is added to the security filtering window, it is being granted these two rights (and vice versa). To see the exact permissions being applied via security filtering (and to get to the security properties of a GPO in general, do the following:

1. Within the GPMC, select the GPO you're interested in and choose the **Delegation** tab in the right-hand pane.
2. Within the Delegation tab, select the **Advanced...** button in the lower right-hand corner.
3. Select the object of interest in the **Group or user names:** pane and look at the permissions assigned in the lower pane.

The following shows an example of what I'm talking about:



You can also manage permissions directly in this window and that's how we used to have to do it before the GPMC came along. But unless you have some specific need to make changes here, it's generally better to simply add/remove objects in the Security Filtering window.

WMI Filtering

WMI stands for Windows Management Instrumentation and it's been created as a way to specify and act on computers based upon chosen characteristics. Examples of this would be computers running the Windows 7 Operating System, computers with a particular brand of motherboard or with a certain size hard drive, etc. In short, it's a way to say "I am only interested in these specific computers". Group Policies allow you to use WMI queries to specify in a very granular way which GPOs will apply to which computers. You'll need to learn how to write a WMI query, but if your environment has a need for this level of granularity, the functionality is present.

To write your own WMI Filter, you'll need to create the filter and then apply it to your GPO of choice. To do this, take the following steps:

1. In the GPMC, right-click the WMI Filters node and select **New...**
2. Give your WMI Filter a name and a description and then select Add.
3. Make sure the Namespace window shows *root\CIMv2* and then type your query in the Query window.
4. Save your query (you will see the query appear in the right-hand pane as well as beneath your WMI Filters node on the left of the GPMC).

Now that the WMI Filter has been created, you can apply it to the GPO of your choice by doing the following:

1. Select the GPO of interest and choose the Scope tab in the right-hand pane.
2. At the bottom of the Scope pane, locate the WMI Filtering section.
3. Select the drop-down box entitled This GPO is linked to the following WMI filter:
4. Choose the WMI filter from the provided list (when you select it, you'll get a pop-up confirming you want to change the WMI filter for this GPO. If you're sure, select Yes).

At this point, the WMI filter is assigned to your GPO and only those computers meeting the specifications of this filter will receive the GPO. Because WMI filtering can become very complex, it is always a good idea to thoroughly test these settings before applying them in production. If the computers which are the target of your filter aren't receiving the GPOs they should, it's likely that the filter has been written wrong.

NOTE: Even if you write a WMI query to include a particular computer object, it will still need to have 'Read' and 'Apply Group Policy' permissions over the GPO in order to apply its settings.

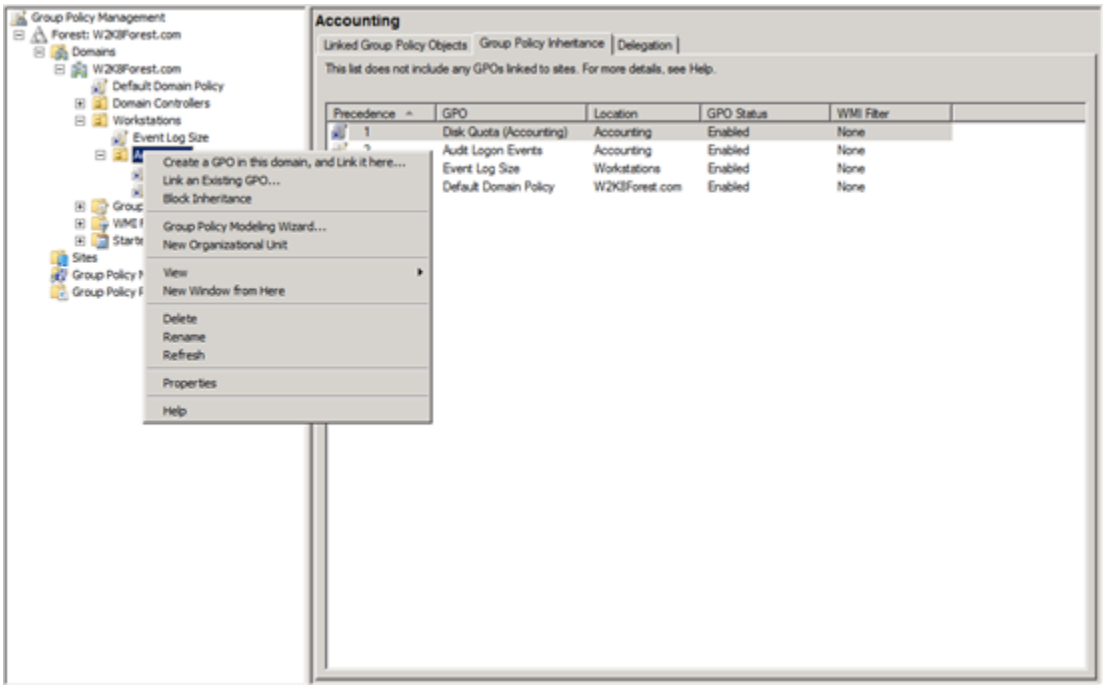
Inheritance, Blocking and Enforcement

The second concept that we need to address is the idea of GPO inheritance and the ways administrators can control whether a higher-level GPO is applied to the objects further down in the directory. This can become especially relevant when you have a large number of GPOs and you don't need the clients within a particular OU to apply all of those settings (applying all of those settings requires more time for your client to start, after all).

Going back to our example above, let's assume that the members of the Accounting OU don't want the *Event Log Size* GPO to apply to their client machines for some reason. Unless something is done to prevent it from applying, its settings will go into effect on client machines in the Accounting OU. You could make the decision to create a second GPO to overwrite the settings in the *Event Log Size* GPO, but then your clients have two GPOs to process, one applying some settings and the other removing those same settings. It seems a bit cumbersome. Thankfully, there's a better way.

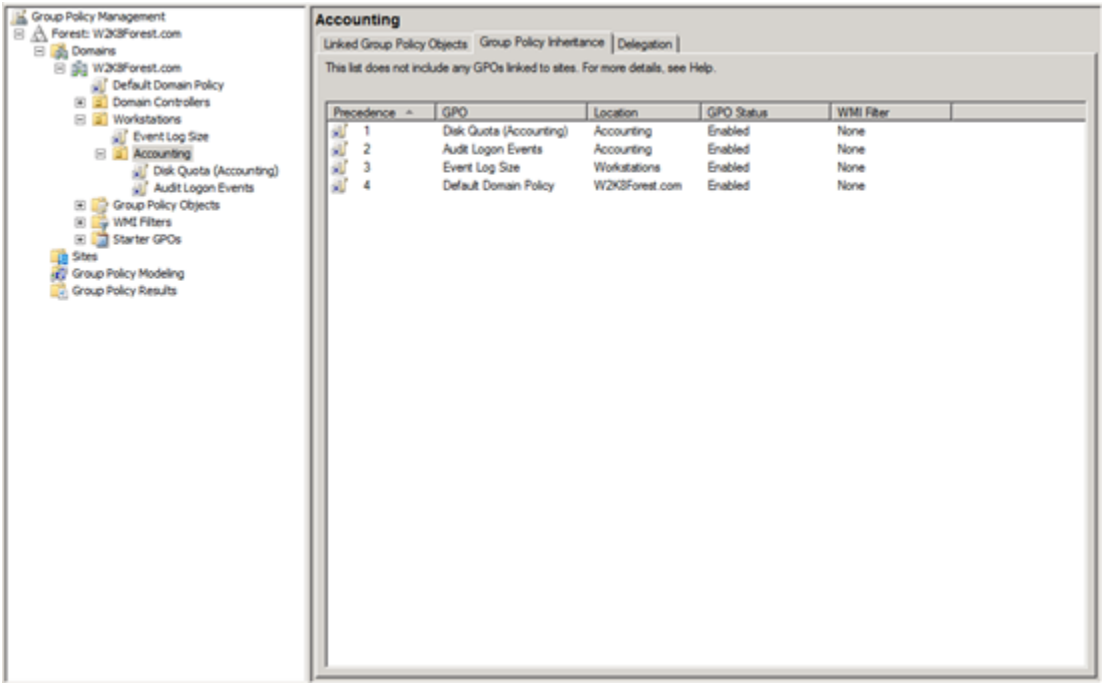
Instead of creating yet another GPO whose purpose is to undo the settings of a higher-level GPO, administrators have the ability to block higher-level GPOs so that they don't apply to your OU. It's important to note that when you choose to block higher-level GPOs, you are blocking all of them. So any GPO that is inherited will no longer apply. Only those GPOs that you configure directly on your local object will apply (if you create child OUs, inheritance will apply to these, starting at the parent OU where the blocking is in effect).

A couple of screenshots should help explain this.



In this screenshot, you can see how to block inheritance of higher-level GPOs. All that is required is for you to right-click the OU (in this case, the Accounting OU) and select **Block Inheritance**. A check will appear beside it and all higher-level GPOs will be blocked from applying within your OU or any child OUs you might configure.

Below, we see a before/after picture of the GPOs that will apply to the Accounting OU:

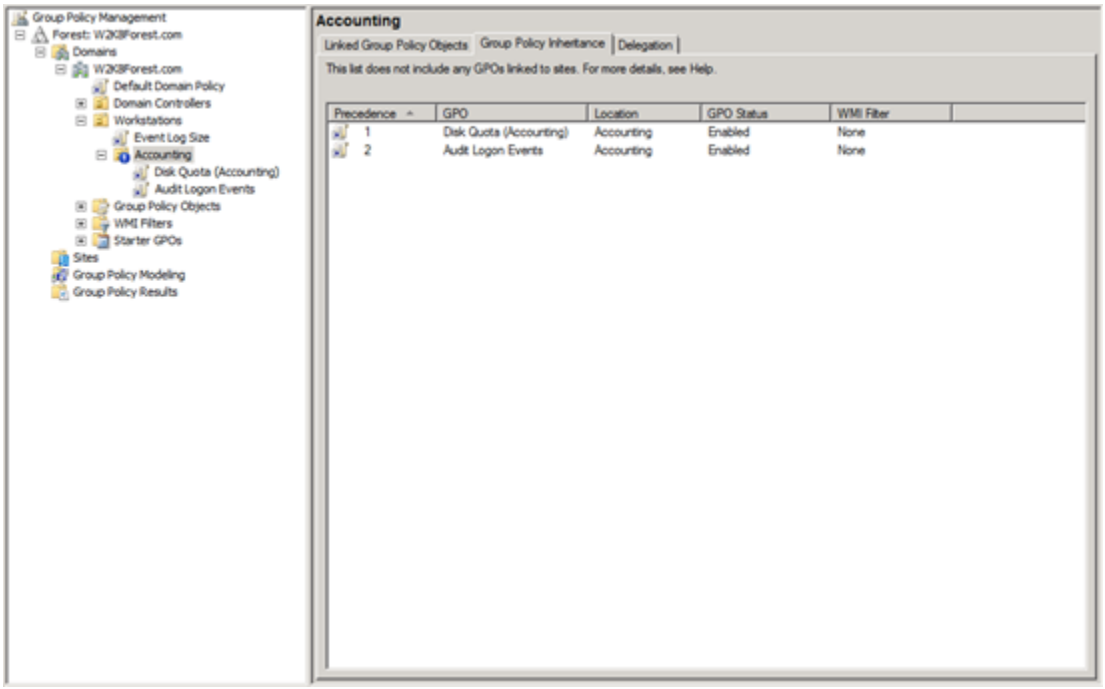


Before we block inheritance at the Accounting OU, we can see that 4 policies will be applied (starting with the bottom and working up). These are:

- Disk Quota (Accounting)
- Audit Logon Events
- Event Log Size
- Default Domain Policy

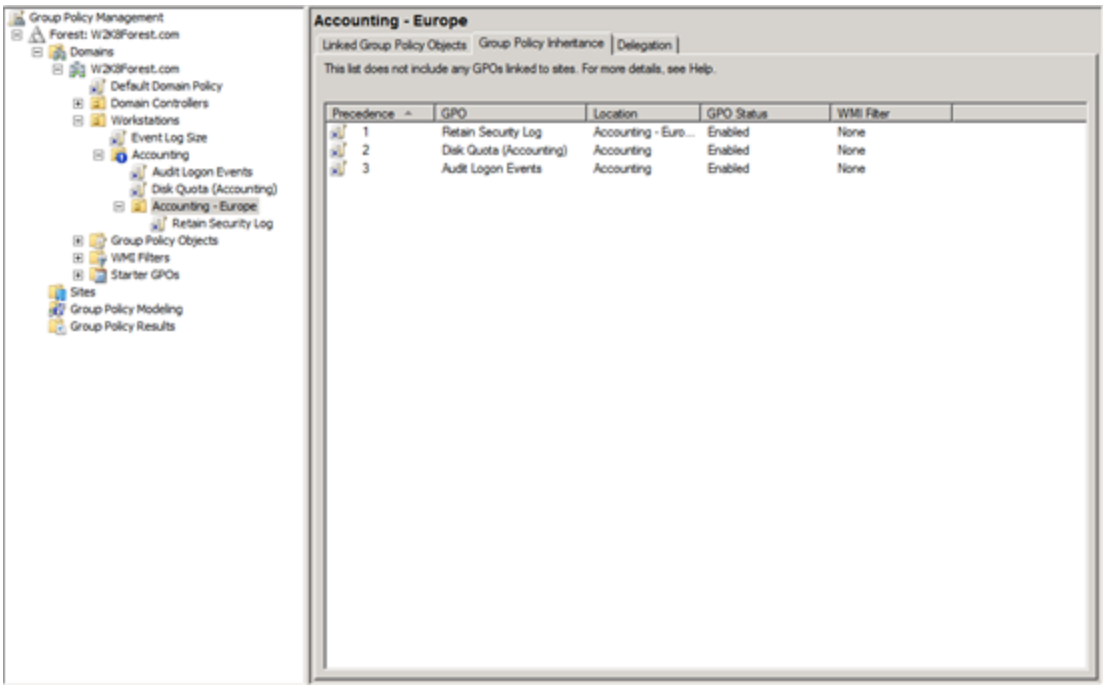
As already mentioned, these policies apply from the bottom to the top. So, for example, if a setting in *Default Domain Policy* conflicts with a setting in *Audit Logon Events*, the setting in *Audit Logon Events* will win.

By contrast, after we set **Block Inheritance**, we can see that the higher-level GPOs no longer apply to the Accounting OU:



Here only the policies specifically defined for the Accounting OU will be applied (again in bottom-to-top order). You will also note that there is now a blue circle with an exclamation point showing next to the Accounting OU. This is how the GPMC notifies you that **Block Inheritance** is in effect.

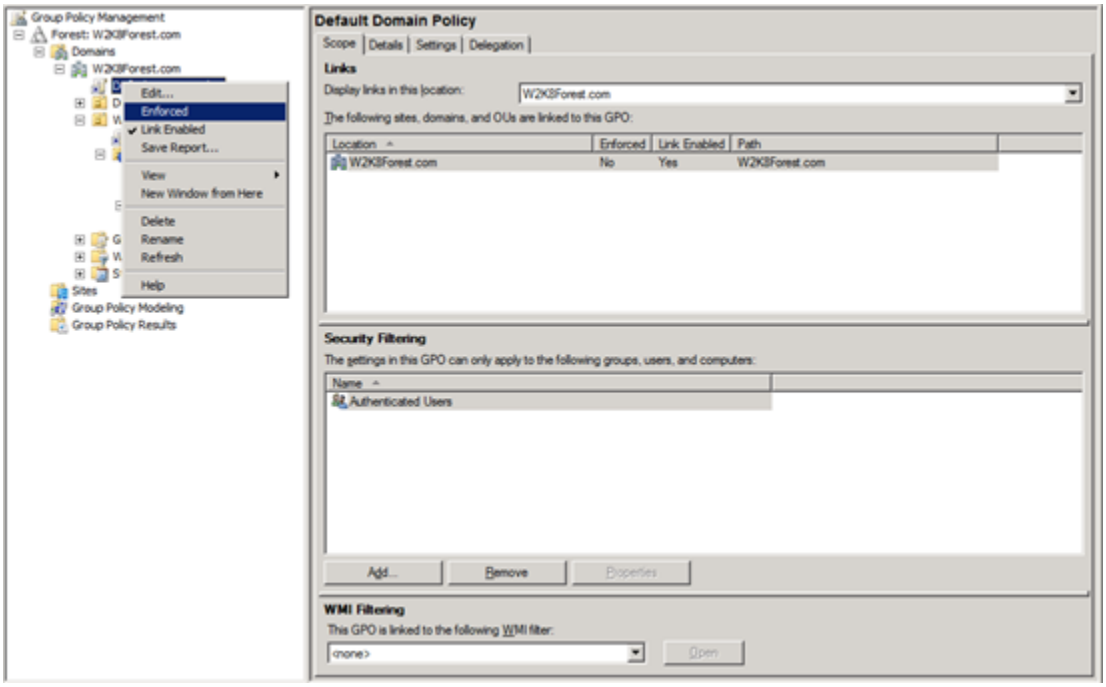
For the sake of clarity, let's look at one final screenshot to clear away any lingering questions. We've said that any inherited GPOs are blocked when Block Inheritance is set. But even with this setting in place, child OUs created beneath the blocking point will still inherit everything from that point on down. In our example, this means that if we create a child OU under the Accounting OU, it will inherit the policies created at the Accounting OU as well as any GPOs linked directly to the child OUs. We can see this in the following screenshot:



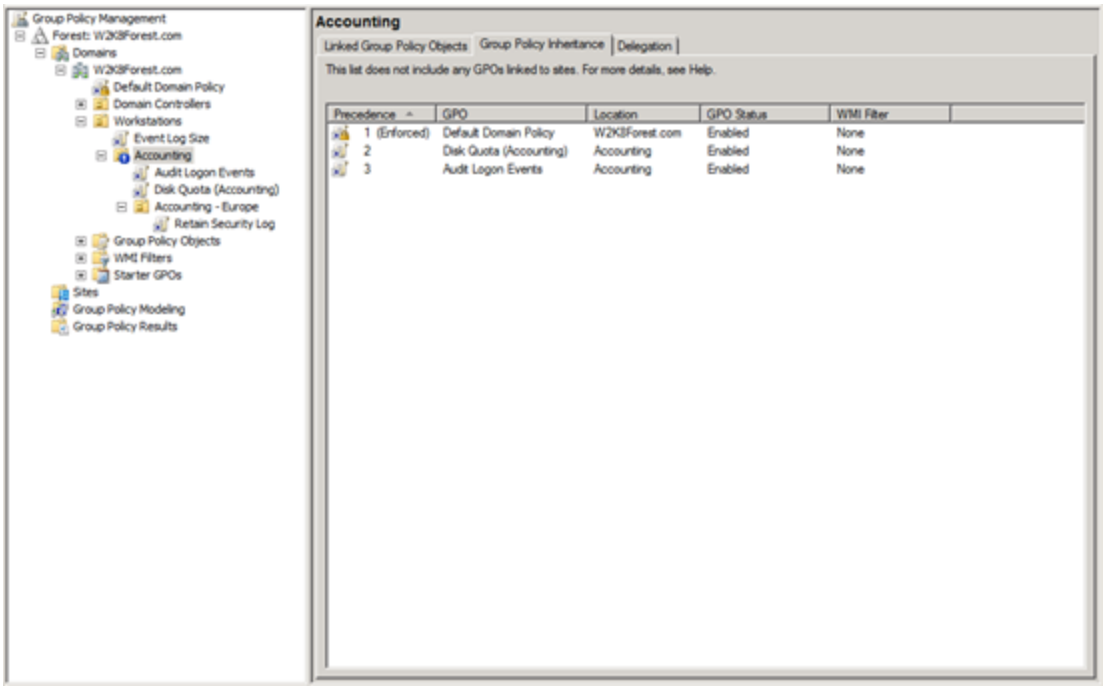
Here you can see that I've created a child OU called Accounting - Europe along with a new GPO called *Retain Security Log* (maybe we've got a security investigation going on in our European office and we have to be sure that security log isn't overwritten). You can see from this screenshot above that, even with **Block Inheritance** set, the GPOs from the Accounting OU (though none above the Accounting OU) still inherit to the Accounting - Europe OU.

Finally, to throw one more bit of complexity into the mix, let's assume that you're the domain administrator and you want to make sure that none of the admins responsible for any of your child OUs is able to block a particular GPO. It turns out that you have the ability to force all of your clients to receive your policies even if they want to block them. This process is called Enforcing.

Looking at the screenshot below, we can see that if we want to enforce a particular policy, we just need to right-click it and choose the **Enforce** option. When we do this, a small lock symbol will appear beside that GPO to let us know it's being enforced.



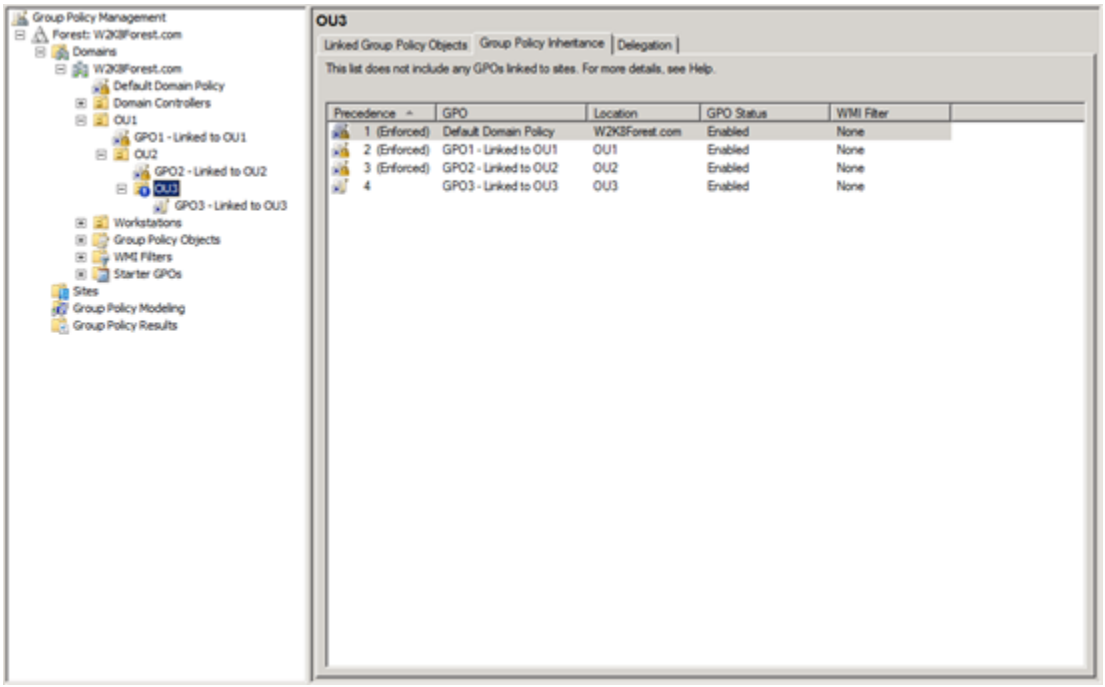
One a GPO is enforced, it overrides any attempts to block it, as we can see below. Here, the Accounting OU still has blocking set but we can now see that the *Default Domain Policy* is once again being processed within that OU. To help us to understand why it's being processed even when blocking is in place, the GPMC lets us that it's being (Enforced).



Before leaving the topic, here are a couple of additional notes about enforcement. First, when a policy is enforced, its settings will be applied last as the screenshot above shows. This means

that it will override even GPOs that are created and linked closer to where the user or computer object is located. If it contains a setting and a GPO closer to the client object contains a conflicting setting, the enforced setting will win.

Second, if you have multiple enforced policies the one higher up the OU tree will have its settings enforced over ones lower in the tree structure. To illustrate this, look at the following screenshot.



What I've done is to create 3 OUs (OU1, OU2 and OU3) and link 1 GPO to each of them as you can see in the left-hand pane. Then I set **Block Inheritance** on OU3 and configured GPO1 and 2 to be **Enforced**. Default Domain Policy is still being enforced from our previous example.

In the screenshot, you can see that the order of precedence is actually reversed from what you would expect (where the GPO closest to the client object is applied last). Instead, these rules apply:

1. GPOs without enforcement set are applied first, using the normal precedence rules
2. GPOs with enforcement set are applied last, with their precedence rules reversed

So we see that even though the GPO named *GPO3 - Linked to OU3* is is applied directly to OU3 it is applied first and will have its settings potentially overwritten by the GPOs applying later. Then *GPO2 - Linked to OU2* is applied followed by *GPO1 - Linked to OU1* and finally Default Domain Policy. If enforcement was not in place, we would expect it to be the exact opposite, but with enforcement in place the rules of precedence are reversed

Resultant Set of Policy

Resultant Set of Policy is the phrase that is used to indicate which policies apply to client machines and users. When the settings of all your GPOs have been sorted out and the system knows which policies need to be applied based on the rules you've put in place, the Resultant Set of Policies is that list of settings. In this section, we're going to spend a bit of time talking about two tools that will help show you what policies will apply to a particular client. One of them even allows you to model which settings will apply before you put them into production, so it serves as a great planning and troubleshooting tool.

GPRESULT

I'll start with GPRESULT because it's been around longer and is the command-line tool you'll use to see which policies are applying to your clients. GPRESULT was originally included as part of the Windows 2000 Resource Kit, but is present by default in both Windows 2003 and 2008. You can read about the various things you can do with this tool by opening a command prompt and typing

gpresult /?

While GPRESULT can be used for a number of things, our purpose here is to use it to generate Resultant Set of Policy data. Specifically, we're going to look at the following combinations of commands:

gpresult /R

By using the /R switch with nothing else, summary data for the various policies and settings will be printed to your command prompt.

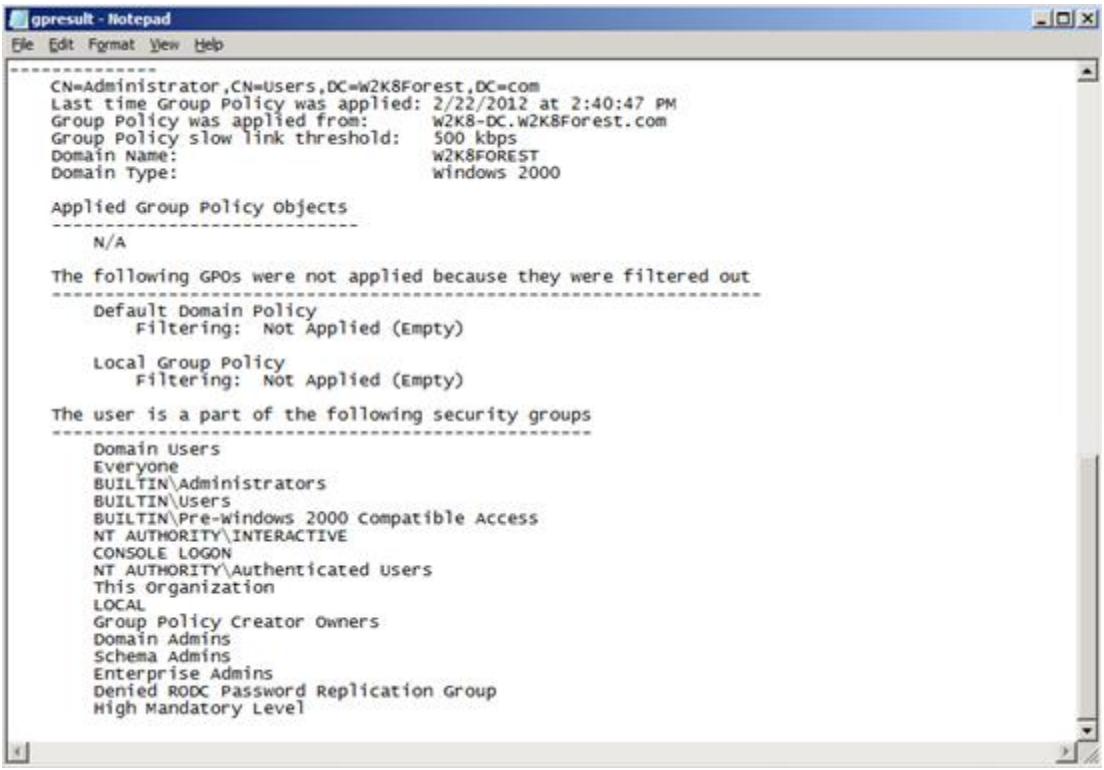
gpresult /V

This is the same as the /R command, only the results will be verbose.

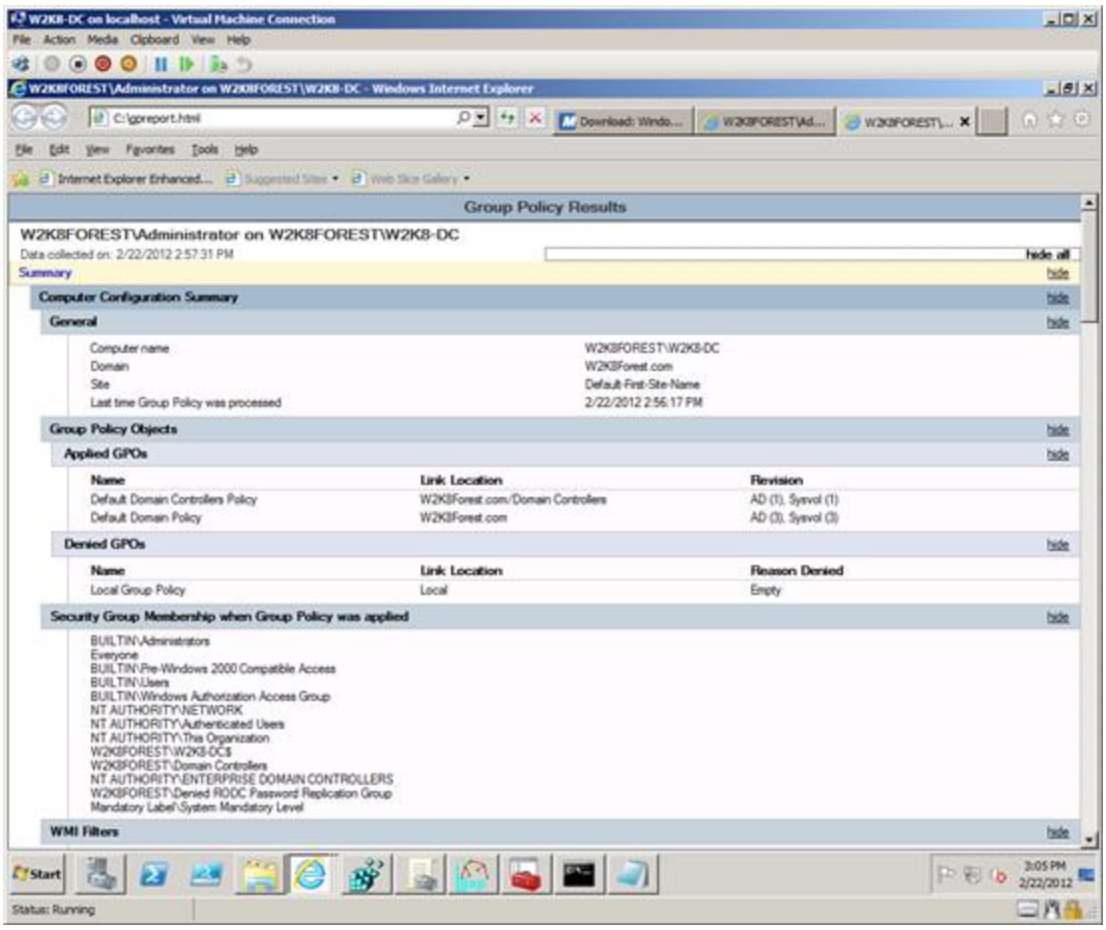
If you don't want all of the settings, you can set the /SCOPE option and choose either USER or COMPUTER, which will result in only the User or Computer node settings being returned.

If you want to save the results to a file, you can do so by either piping the results to a text file using a command similar to *gpresult /R>c:\gpresult.txt*. Another option is to create your output in HTML format by typing *gpresult /H <filename.html>*.

Below are sample outputs in both the .txt and .html formats



GPResult.txt



GPResult.html

Resultant Set of Policy (RSOP)

The newer tool that's been created specifically to see Resultant Set of Policy for your client is called, oddly enough, Resultant Set of Policy. You access this tool by taking the following steps:

1. From your client machine, go to **Start/Run** and open a blank MMC by typing **mmc.exe.**
2. Within the blank MMC console go to File and choose **Add/Remove Snap-in....**
3. From the Add or Remove Snap-ins window, scroll down until you see the Resultant Set of Policy snap-in. Highlight it and select the **Add** button.

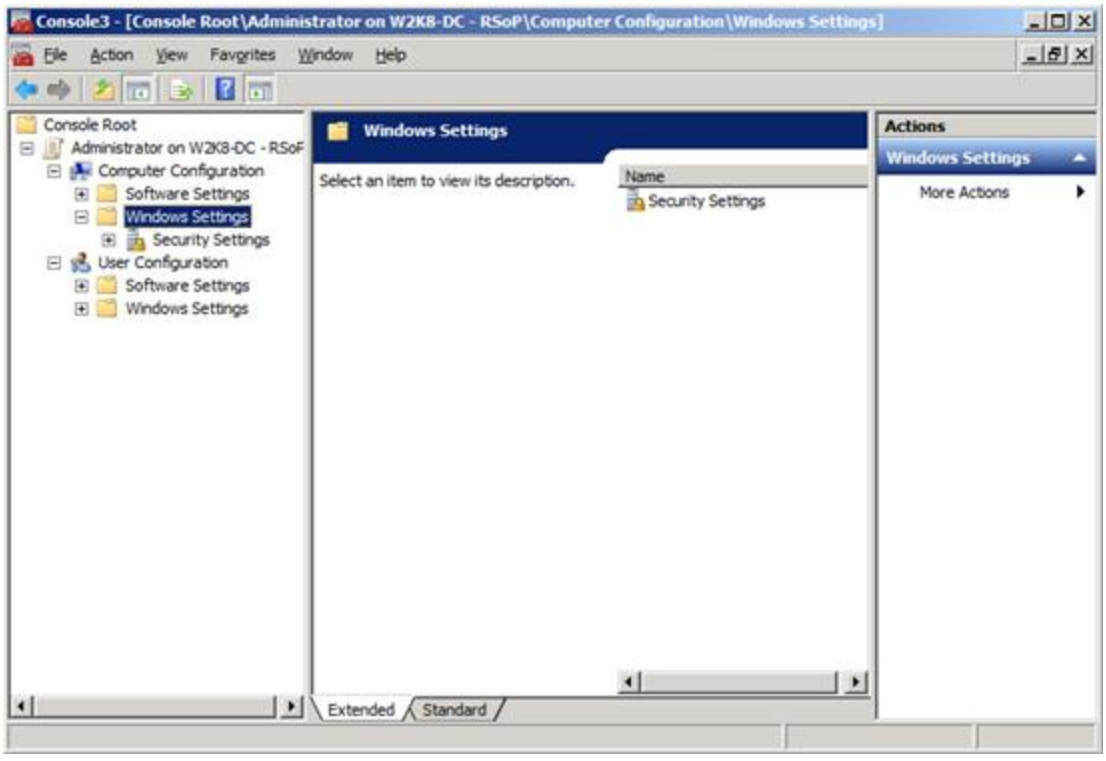
Select OK and you'll be looking at the Resultant Set of Policy tool. Not much shows in the window at first, but we'll quickly change that. To see policy settings, the tool will need to gather data. It does this through a wizard that is started when you select **Action** from the menu bar and choose **Generate RSoP Data...**

When generating your RSoP Data, you can choose Logging or Planning mode. If you choose Planning mode, the system will show you what settings would apply if an object were located at a particular place in your directory structure. This is a great "what if" tool in cases where you're

considering migrating objects to new containers within Active Directory and you want to know what effect this will have on them from a Group Policy perspective. Planning mode is also great in a test environment where you've configured the directory and GPO structure that you think will do what you need. Using this tool, you can generate the resultant set of policy which will show you the settings that will take effect on your client objects. If the settings aren't what you expect, you can make the necessary changes and test again.

The other way to use the Resultant Set of Policy tool is in Logging mode. This mode will review the settings currently being applied to a particular computer or user (or both). You can select either the local computer or a remote device and when the wizard runs the results will display the resultant policy settings that are applying to that device. This is especially useful when you're trying to understand whether a particular setting should be applying to a computer or user. If RSOP doesn't show the setting, it may mean something has happened in your GPO implementation that is preventing that setting from taking effect.

A screenshot of what the RSOP tool looks like is below:



Resultant Set of Policy is a powerful tool that is especially useful in understanding ahead of time what settings will apply to objects before you make modifications to your directory. It is also very useful as a diagnostic and troubleshooting tool (though I personally prefer GPRESULT since I don't have to drill down through as many containers if I'm looking at the report in the command line or a text file).

Summary

So now you should understand how a GPO determines which GPOs it should process and how to find them (through the gPLink attribute). You should also understand the order in which they are processed, how decisions are made about which policy settings to apply when there are conflicts, and how to block and enforce settings within your environment. I also showed how to use a couple of tools to see which policies should be applying to your GPOs, which will be helpful to you when understanding and troubleshooting policies in your environment.