# Group Policy Objects: What are They and How Can They Help Your Firm?

By Sharon Nelson and John Simek

The obvious first question: What is a Group Policy Object? Basically, a Group Policy Object (GPO) is a policy to define user and computer configurations in a Windows environment. You can configure a GPO at the site level, domain level or OU (Organizational Unit) level. They work by forcibly setting user and computer registry values. Since almost all of a Windows computer system is controlled through the registry, you have a lot of options when setting these policies. We'll attempt to give you some examples of common usages for GPOs and even some standard controls that should be implemented in every law firm.

If reading paragraph one has already caused your eyes to glaze over, be forewarned that this is not a sexy topic – one reason why you don't see too many articles about GPOs. But they are doggone useful, so get yourself a double shot of espresso and read slowly to get information you really can use in your law practice.

Can you control and restrict a Mac computer with a GPO or is this only for Windows systems? The simple answer is that it is much more difficult and complicated to achieve the same types of control and configuration for a Mac than it is with the embedded capabilities of a Windows computer. One solution is to integrate Open Directory with Active Directory. This requires a Mac OS X Server, which a lot of firms don't have. To make matters worse, Apple has announced that it is discontinuing its Xserve product line and may stop producing other server products. Another option is to purchase a third party product like DirectControl from Centrify.

We'll talk about using GPOs in a domain environment, which means you are running a Windows server on your network. Many of the things we'll mention are also available for stand-alone computers running XP, Vista or Windows 7. Obviously, if you have a server-based environment, the preference is to centrally manage users, computers and applications. It is much more time and cost effective to centrally manage Group Policies through Active Directory than it would be to run around to every computer and set the local policy. These Active Directory based GPOs are also known as nonlocal GPOs. They are created in Active Directory and stored on a domain controller, such as a Windows 2000, 2003 or 2008 server.

## Tools

How do you create and manage a GPO? For Windows Server 2000 and 2003 domains, you would use the Group Policy Object Editor from the Active Directory Users and Computers console following these steps:

1. Click Start, Administrative Tools, and click Active Directory Users and Computer.
2. In the console tree, locate and right-click the domain (or OU) to which you want to link a GPO, and click Properties on the shortcut menu.

3. When the Properties dialog box for the domain opens, click the Group Policy tab.
4. In the Group Policy Object Links list, click New and then click Edit to create a new GPO, or choose an existing GPO in the Group Policy Object Links list, and then click Edit.
5. The Group Policy Object Editor opens for the domain GPO.

It's a little bit different if you are running a Windows 2008 domain.

1. Click Start, All Programs, Administrative Tools and then the Group Policy Management icon.
2. Expand the domain name.
3. Expand Group Policy Objects.

Generally, you will edit the default domain policy. Windows 2008 domains also have a default Domain Controllers Policy. The default domain policy already has a lot of built-in objects that can be edited very easily.

Group policies can become very complicated, especially in larger environments. You will want to be familiar with the Group Policy Results (GPResult.exe) command line tool to troubleshoot Group Policies implementations. You start by opening a command window. This is done by:

1. Click Start, Run and enter cmd to open a command window.

Typing gpresult in the command window will show you all of the optional parameters that are available. A very common entry would be gpresult /r to generate a report to the command window. The report will show such things as the operating system that is running and any policies that are in effect.

## Policy Inheritance

A large number of problems with GPO implementations arise from a lack of understanding about inheritance. You do have the option of blocking inheritance, but we think that makes the situation even worse. If you leave the default inheritance enabled, then you can just follow the flow through the Active Directory "tree" to see where the problem may lie.

GPOs inherited from the Active Directory are always applied over the local policy. Even if a user has administrative rights to their computer, an administrator can overwrite anything they configure through the use of a domain policy. After that, the GPO that is closer to the object (e.g. computer) is "stronger" and takes precedence.

## Policy Updates

Group Polices from Active Directory are refreshed on the computers by several methods:

1. Logon to the computer (if the GPO settings are "user settings").
2. Restart of the computer (if the GPO settings are "computer settings").
3. Every 60 to 90 minutes when the computer queries the Domain Controller for updates.
4. Manually by using the gpudate command (Windows 2000 uses the secedit command).

Generally you will want to manually force the GPO updates while you are configuring and testing the policies. As an example, if you configured a GPO for a printer installation (yes you can do that), you would want to see if you got it right. Configure the GPO, force the update and then see if it actually works.

## Types of Control

GPOs can do a lot to automate activity and control configurations of your computers. Some of the things that can be achieved are:

1. Configure the user’s desktop. This could include all sorts of things like device (e.g. printer) installations, colors, etc.
2. Configure local security on computers. You can restrict access to specific folders on the machine or whether the last logon name appears.
3. Install applications. This is a great activity, especially for deploying new applications to a bunch of computers or sending out updates. Besides installations, you can also remove the icons and ability to run certain programs like the built-in games that come with Windows.
4. Run startup/shutdown or logon/logoff scripts. You can have certain activities occur when the machine is started or shut down. As an example, all temporary files can be cleared when a user logs off the computer.
5. Configure Internet Explorer settings. You can set a default home page for the user’s browser.
6. Redirect special folders. You can assign drive letters to specific folders.

## Common GPOs

Now we’ll get to the more interesting items that you’ve been waiting for. We implement GPOs for the majority of our clients and even do some special activities as they request. Several of the GPOs we implement are for security and confidentiality reasons. The rest of them tend to be for application management or standardization within the firm.

## Last Logon ID

One of the GPOs we highly recommend is removing the display of the last user ID that logged onto the computer. Typically, you will logon to a computer using a user name and a password. By default, Windows will leave the user name populated with the last ID that was used to logon to the computer. This means that only one more piece of information (the password) is needed to gain access to the computer and therefore data on the network. By removing the display of the last logged on user, two pieces of information (user ID and password) are needed. This makes it harder for someone to compromise your systems since they’ll need both items for a successful logon.

## Password Length

Another object we define is password length. At the present time, passwords that are at least 8 characters in length are required. With the recent password cracking results from the Georgia Institute of Technology, 12 character passwords should now be required.

## Password Expiration

Passwords should expire after a period of time, thereby requiring that they be reset. You're familiar with this concept if you do any online banking. Periodic password changes help maintain security of the system. We set the password expiration at 30-45 days.

## Password History

This value defines how much time must pass before you can reuse a password. This is to prevent a user from changing the password (because it expired) and then changing it back to the old value. That would defeat the purpose of the expiration period. We set this value at 24 months, which means we will never see the same password being used for at least two years. Some users will object to this policy and complain that they can't remember their passwords. Resist the temptation to soften this policy. Perhaps changing the expiration period to a longer time would be a good compromise.

## Account Lockout

There are several GPOs that can be set for this. The Account Lockout Threshold is the number of times an incorrect user ID/password can be typed in before the account is locked out. A number between 3 and 5 should be sufficient to account for honest mistakes and typographical errors. The Account Lockout Threshold is important to stop attempts by a computer program or person trying to gain access to your computer systems.

The Lockout Duration is the period of time that the account remains locked following the number of invalid logon attempts as set by the Threshold value. If you use a value of zero, the account will remain locked until it is manually unlocked by the administrator. A Lockout Duration of 30-60 minutes is an acceptable period. This will be sufficient to stop hackers or botnet computers from guessing user ID and password combinations.

## Folder Redirection

This is the GPO where the system folder contents for the user are redirected to a central storage area on the server. This allows the user to use any computer and have their information stay consistent. Examples of the types of folder redirection contain the following:

- *Application Data:* This folder contains the user configuration files, the user specific data that is utilized by applications and PKI files. By redirecting this folder, the user does not need to be configured again when they change systems. Their applications will work in exactly the same way no matter which computer they use.
- *Desktop:* This folder contains the files and shortcuts that appear on the user's desktop.
- *My Documents:* This folder contains the files and pictures for the user. This means the user can access any of these files from any computer.
- *Start Menu:* This folder contains the shortcuts and files that appear on the Start menu.

## Temporary Files

Several of our clients want to clear the temporary Internet files for each user. We configure a GPO to clear the temporary Internet files when each user logs off.

## Internet Explorer Home Page

Some firms want consistency with their workstations. One of the GPOs we implement changes the default home page for each user's Internet Explorer home page. The firms typically set the home page to be the home page for the firm. So if an associate changes the home page to CNN, too bad. The next time they logon and launch Internet Explorer they're right back to the firm's home page. This is because the GPO will override the user change.

## Application Deployment

A very valuable feature of GPOs is the deployment of applications. We're used this ability to roll out new versions of Office to every computer, distribute the anti-virus software and quickly distribute any software or patches within the firm. It takes a little work to configure and test a GPO so there should be several computers that need distribution before expending the effort. As an example, it's probably not worth implementing a GPO to distribute QuickBooks to one computer. However, pushing out an update for Tabs3 to 13 computers is worth it.

## Summary

We've identified some of the common uses for GPOs. Hopefully, you have an appreciation for how they can benefit your firm. GPOs can get complicated so make sure you are comfortable with the tools available for troubleshooting. The nice part about GPOs is that you can just disable one that isn't quite working right for you and troubleshoot it later.

Clearly, GPOs are not for the faint of heart. For most lawyers, if they wish to achieve some of the results described above, they are better served by utilizing their IT staff or IT consultant. But GPOs are invaluable – they offer consistency, save time/money and provide many levels of security. As you can see, it is well worth your time to gain at least a primitive understanding of GPOs.

*The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, information security and computer forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com*