Group Policy Basics - Part 1: Understanding the Structure of a Group Policy Object

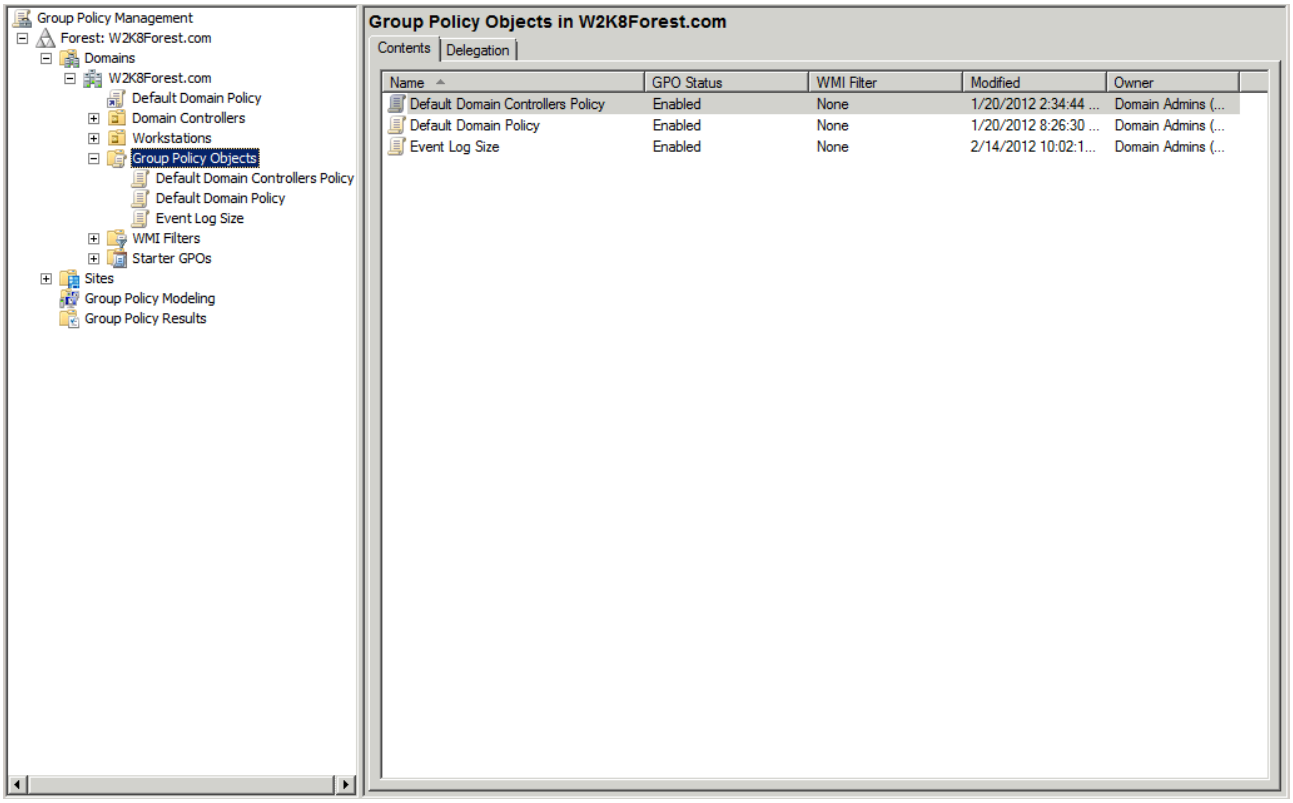
By kexugit

Archived: 2026-04-06 00:02:55 UTC

As a Windows administrator, you almost certainly have used Group Policies to control the settings deployed to the clients of your Active Directory infrastructure. But with Group Policies getting such heavy use, not as many administrators fully understand how Group Policy Objects (GPOs) are structured. In this post, I will discuss the structure of GPOs in order to help bring greater understanding to this topic. When you're troubleshooting Group Policies in your environment, it's helpful to understand how they're structured, and hopefully this post will clear up a bit of that mystery.

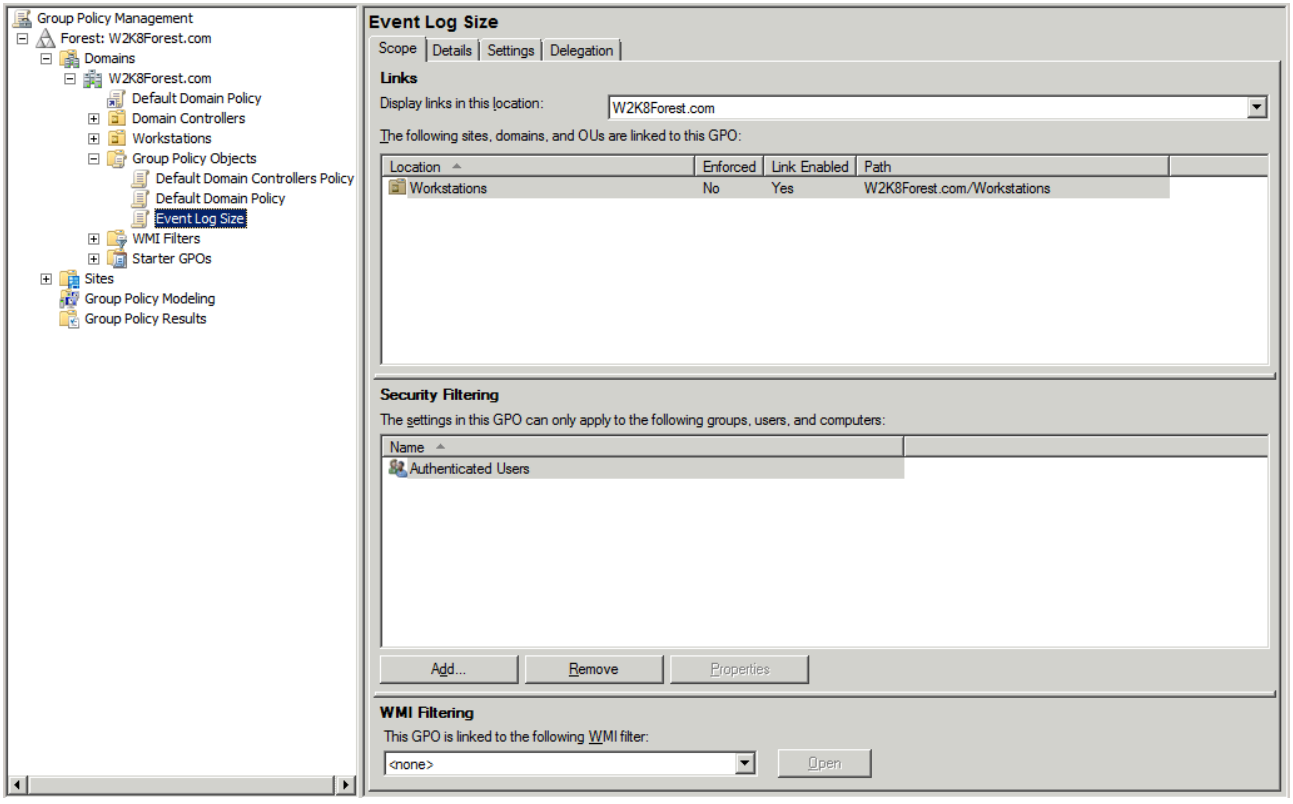
Group Policy Objects are actually composed of two parts, the Group Policy Container (GPC) which exists in Active Directory and the Group Policy Template (GPT) where the actual content of your GPOs resides. A third component, known as Client-Side Extensions (CSEs) can be found on client devices and are necessary for them to properly process the Group Policies assigned to them.

Before we go through these individual pieces, take a look at how GPOs show up when viewed through the Group Policy Management Console (GPMC).



In the early days of Active Directory, the only real way to get to a GPO is to open the location where it was linked (a domain, organizational unit, or site). This made it appear that the GPOs existed at those place in the directory when they were actually only linked to those locations so that their settings would apply to the specified objects they contained (such as the computer objects within a particular OU). With the GPMC, it's much clearer to see that GPOs do not reside at these different points of the directory but instead exist separately and are only linked to these different levels.

To see an example of where a GPO is linked, you can check the Scope tab of your selected GPO within the GPMC, as shown below.



You can see from this picture that the GPO I created named *Event Log Size* is linked to the Workstations OU within the W2K8Forest domain. You can further see that the link is enabled (meaning the policy will apply), but it is not enforced (meaning that the policy can be blocked if the administrator of the Workstations OU wishes to prevent the policy applying).

But even the GPMC's view of where GPOs reside is a bit misleading as there really is no Group Policy Object container in Active Directory. Instead, the actual structure of the GPO is laid out as follows.

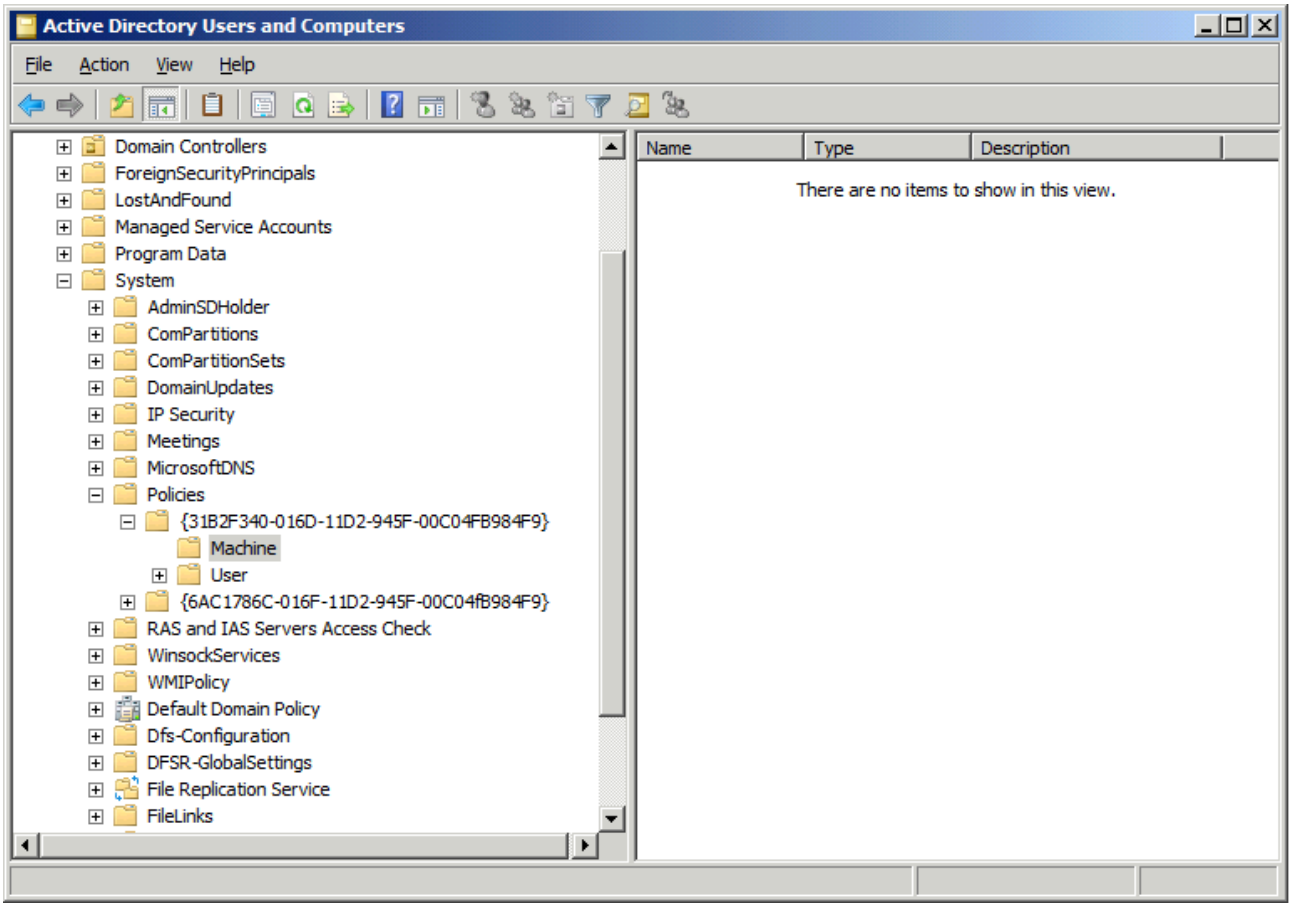
Group Policy Container (GPC)

The first piece of the GPO, while not within a container called Group Plicy Objects, is still found within Active Directory. In order to see it, there are several options. The most common is to use Active Directory Users and Computers. If you choose this tool, you'll need to take the following steps to see the appropriate folder:

1. Open **Active Directory Users and Computers** (you can do this by typing DSA.MSC at **Start/Run**)
2. Select **View** from the menu bar and ensure **Advanced Features** is selected (if not, select it)

3. Expand the **System** container and navigate to the **Policies** container

If you don't enable Advanced Features, you won't see the System container. But after this is enabled, you should have a screen similar to the one below:



Notice that there are two containers, each with a string of numbers. Each of these represents a different GPO (the string of numbers is the Globally Unique Identifier, or GUID, of each GPO). Within each of these containers you'll see a Machine and User container. These contain specific information related to the User and Machine nodes of the GPO itself (as you might expect, the Machine node refers to computer settings and the User node refers to user settings).

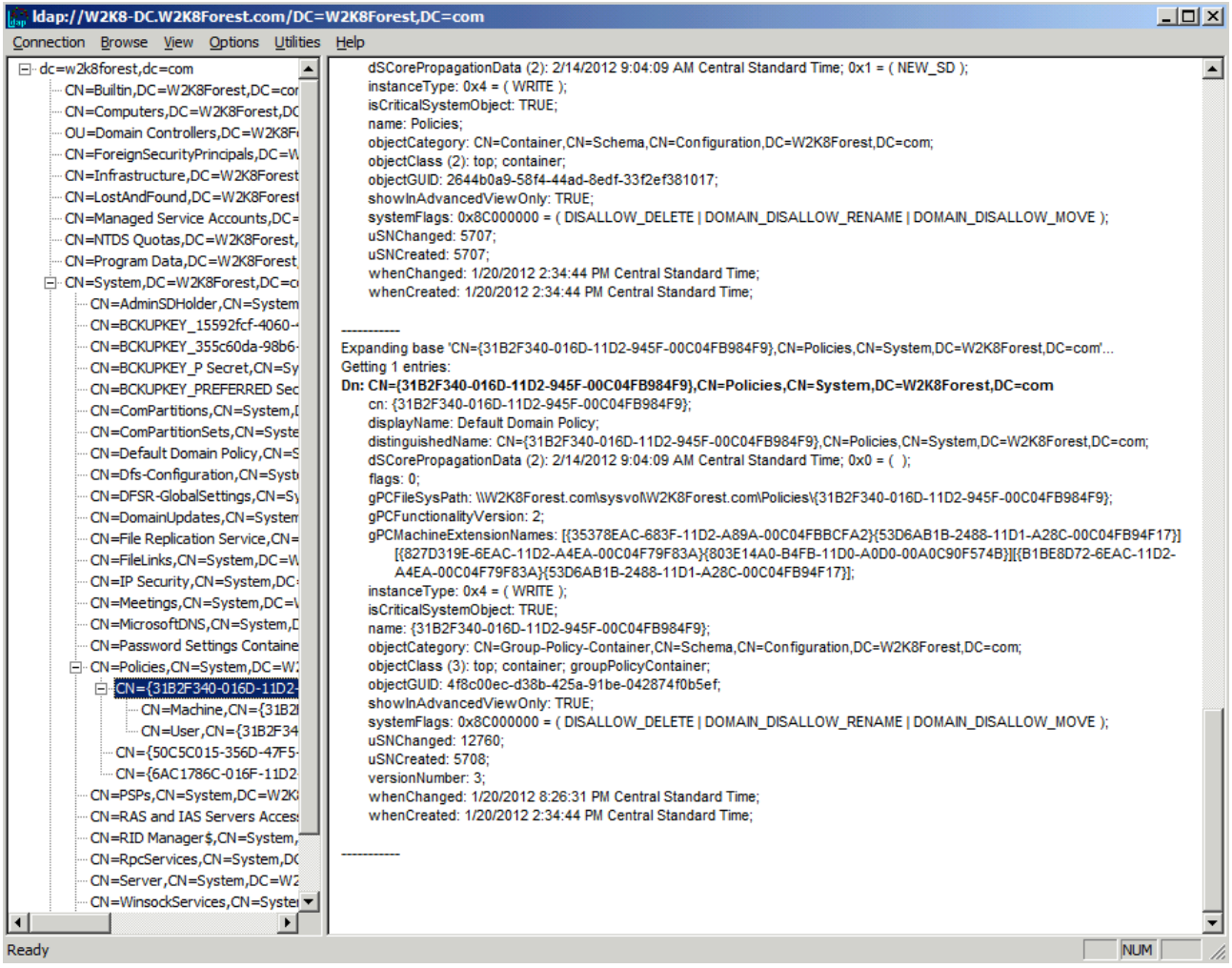
Another tool that you can use to view these folders is LDP. To use LDP to see these folders, take the following steps:

1. Start LDP by typing LDP.EXE at **Start/Run**
2. Select **Connections** from the menu bar and select **Connect...** to connect to the Domain Controller of your choice. Select **OK**
    1. enter the fully qualified domain name of the Domain Controller
    2. enter port 389 since you're doing an LDAP query
3. Select **Connections** again and choose **Bind...**
    1. Make sure you are binding to the directory with an account that has sufficient permissions to do an LDAP query

4. Select **View** and choose **Tree**. Enter the distinguished name of your domain (for example: *dc=W2K8Forest,dc=com*). Select **OK**
5. In the left-hand column, expand the directory tree and navigate to Policies under the System container

There is one big difference when using LDP, which becomes immediately obvious after selecting one of the GPO nodes. When you double-click it, you will suddenly see a great deal of information in the right-hand pane. This is the critical directory information that client machines use when processing GPOs. These settings allow clients to understand where the content of the policy is, which Client-Side Extensions will be needed to process the GPO content, etc.

Here is a screenshot of what you'll see within the LDP window:

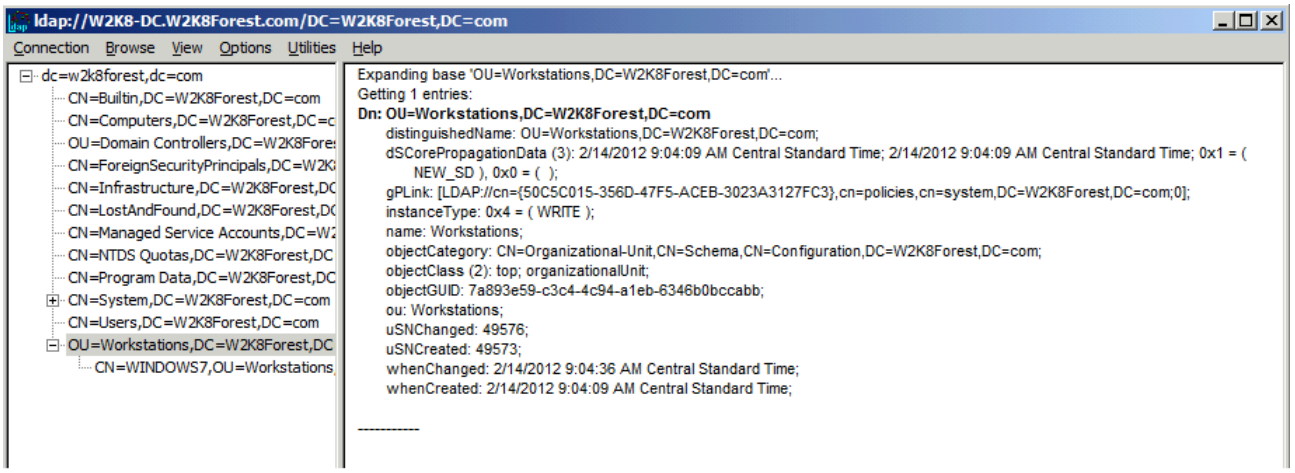


Looking at the details of our selected GPO, there are several attributes which are of special interest to us:

- ***displayName***: This attribute is the human-friendly name of your GPO
- ***gPCFileSysPath***: This attribute points clients to the location where the GPO content can be found. Collectively, this is known as the Group Policy Template, which is housed in a share known as SYSVOL
- ***gPCMachineExtensionNames***: Here is the list of Client-Side Extensions (CSEs) that will be needed by the client in order to process all of the machine-side settings configured for this GPO

- ***gPCUserExtensionNames***: This attribute contains the list of CSEs that will be needed to process the user-side settings. As there are no user-side settings configured in this GPO, the attribute is not populated (and thus not displayed)

Another important attribute is gPLink and while it's not found as part of the GPO itself, you can find this attribute everywhere that the GPO is linked. This allows objects within these other containers to know that there is a GPO it needs to process. In the screenshot below, you can see that the gPLink attribute points to a single GPO found within the policies container of the system partition:



So now we've seen the Active Directory portion of the Group Policy object. It contains settings so that the client can learn which GPOs it must process, which tools it will need to process them, and how to locate the GPO contents in order to process. Now that we've seen the first part, let's take a look at how and where the GPO content itself is stored.

Group Policy Template (GPT)

The Group Policy Template is where the meat of the GPO resides. By way of comparison, think of how Active Directory represents a computer object. It lists all the relevant attributes of the computer, but the object in Active Directory is not the computer itself. In a similar way, the portion of the GPO in Active Directory merely represents the attributes relevant to the GPO content. The content itself is known as the Group Policy Template, or GPT, and it resides in a share known as SYSVOL. This share, like the portion of the GPO stored in Active Directory, is replicated to every DC in the domain. This way, when a client queries for the GPOs it needs to process, it can locate the contents of those GPOs on the same (in most cases) DC where it's conducting the query.

NOTE: The only exception to this rule is cross-domain GPOs where a GPO is defined in another domain, but is linked in such a way that clients from neighboring domains need to apply them (a Site-level GPO is an example, since Active Directory Sites can span multiple domains). In the case of a cross-domain GPO, the client will need to pull content from a DC in the neighboring domain which can be a very slow process. For this reason, cross-domain GPOs are not generally recommended.

To see the content of your GPOs, you'll want to look at the SYSVOL share on one of your DCs. You can find the SYSVOL share by navigating to %windir%/sysvol/sysvol (yes, there is a shared SYSVOL folder within a parent

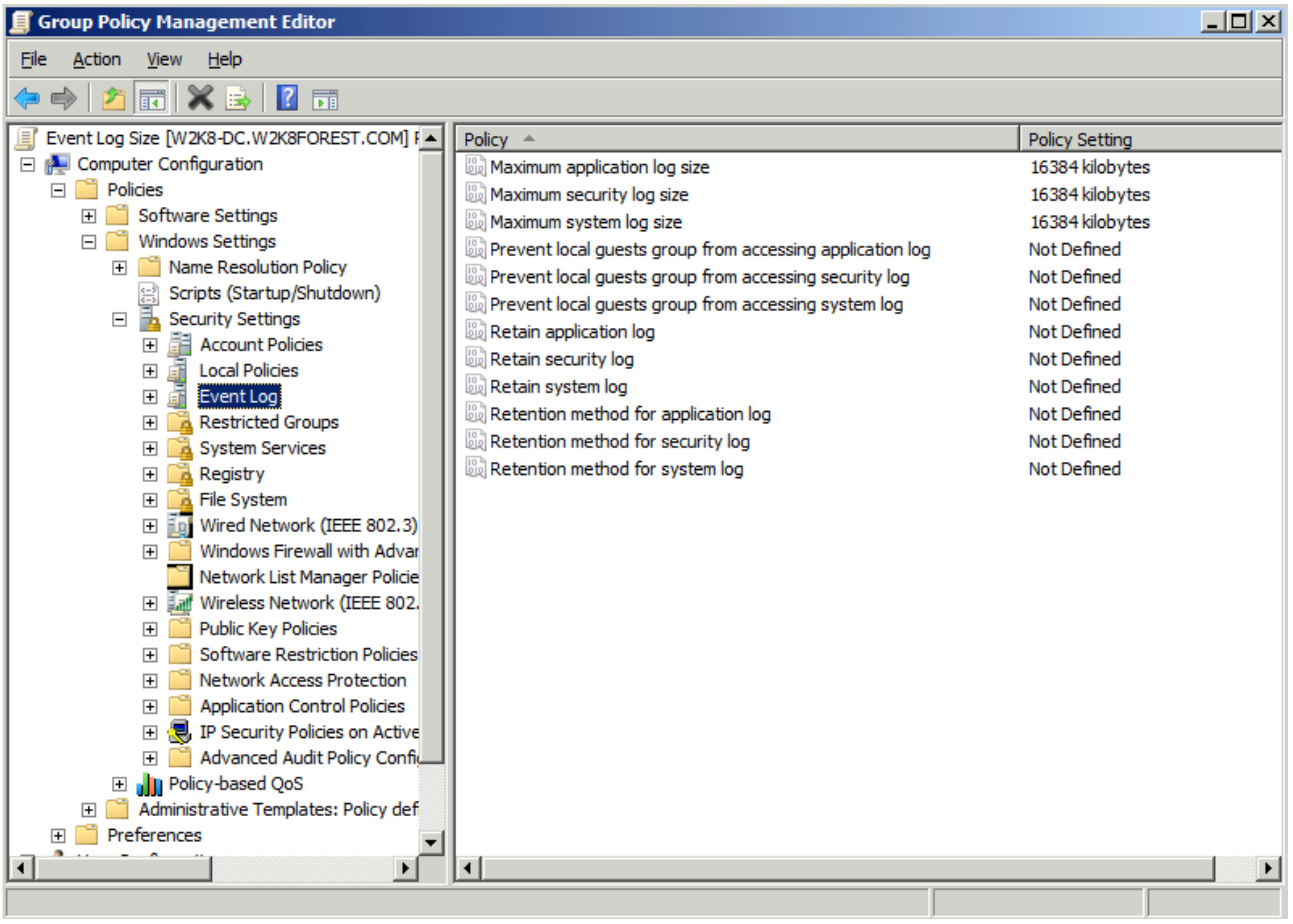
SYSVOL folder). The actual sysvol share is set to **<servername>\sysvol** Within this folder, you will see the same list of GPOs that appear within Active Directory's System/Policies container. These folders are where the actual settings of your GPO are contained. Depending on the number of settings you've put in place, there will be more or less present in each folder. Regardless, you are guaranteed to have at least the following folders/files within each of your GPOs:

- %windir%
    - sysvol
        - sysvol (*shared as **servername****sysvol*)
            - <domain name>
                - Policies
                - scripts

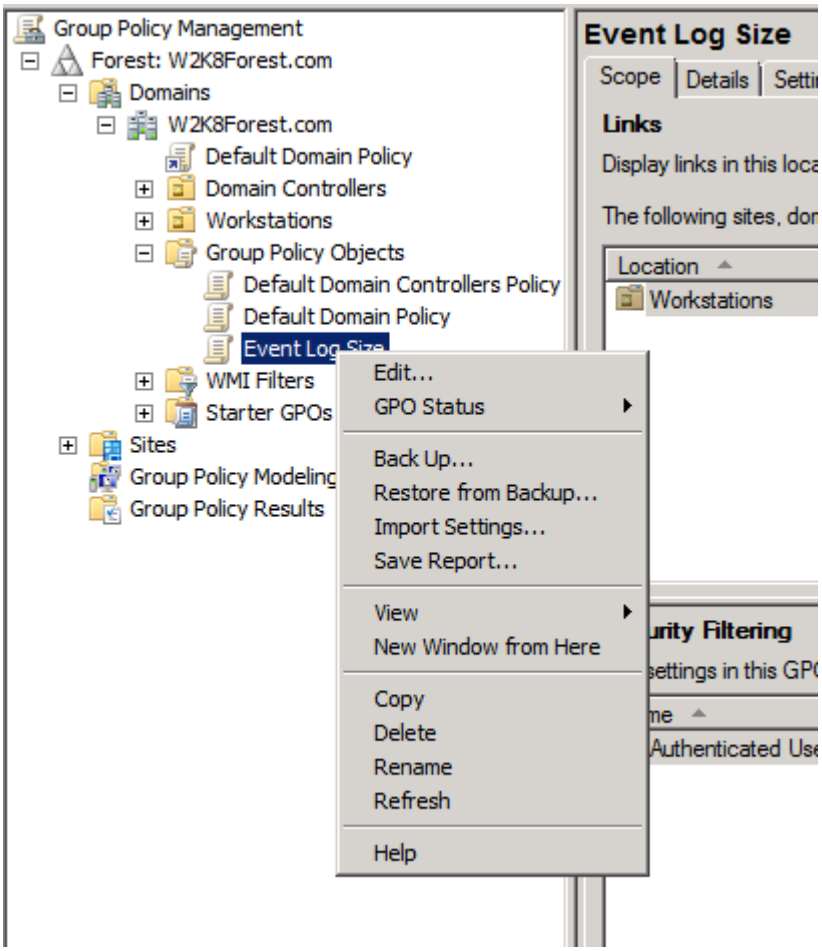
Within the policies folder, you'll find the various GPOs and their configured settings. Again, the following folders/files are guaranteed to be present for every GPO in your domain:

- Policies
    - <GPO GUID>
        - Machine (*folder containing the computer-side settings of the GPO*)
        - User (*folder containing the user-side settings of the GPO*)
        - GPT.INI (*file containing the GPO's configuration settings*)

Depending on what you've configured, the Machine and User folders may or may not contain additional content. As an illustration, lets take a look at the contents of a GPO I've configured to set the various Event Logs on my clients to their maximum size. First, here is the Group Policy Management Editor showing the settings I've configured. This is the tool you'll be working with when you configure the settings for your own environment.

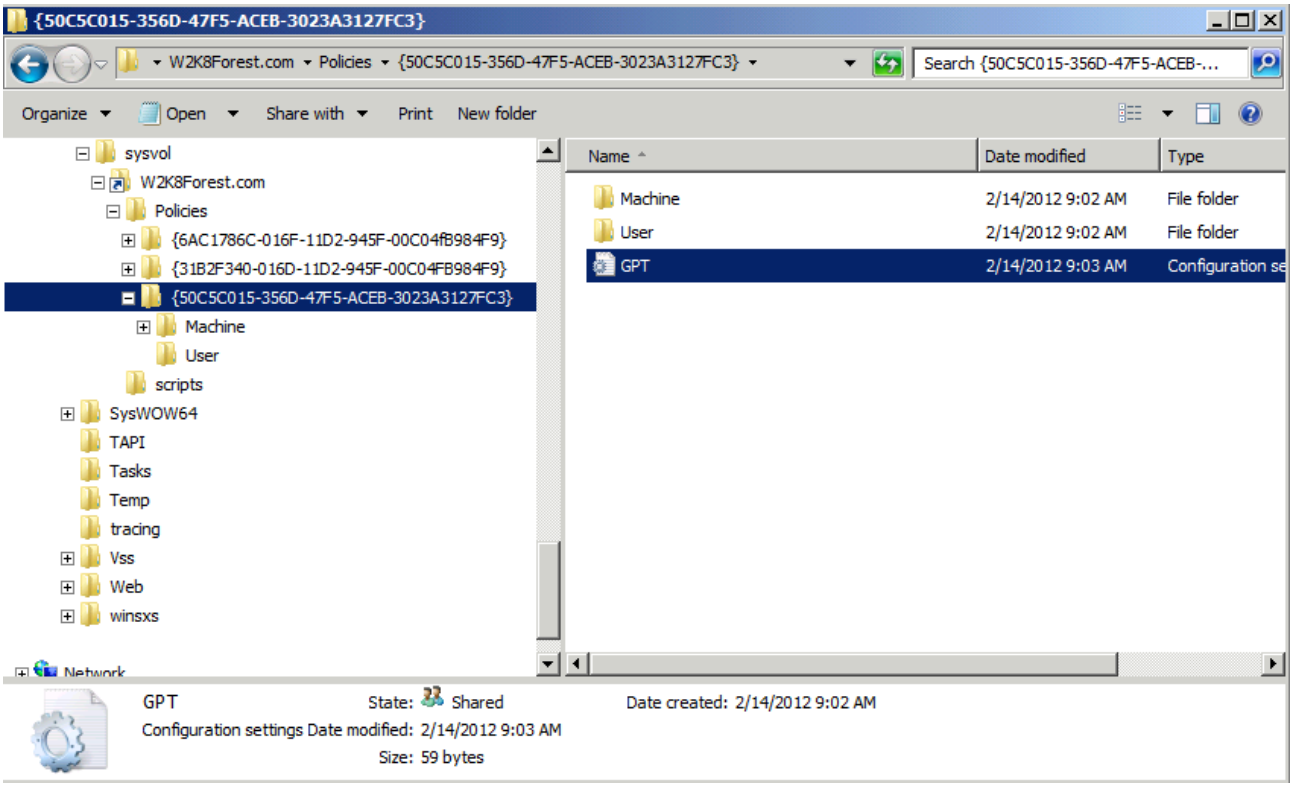


If you need to know how to launch this tool, you do so from within the Group Policy Management Console by right-clicking your GPO and selecting **Edit...** as shown below.

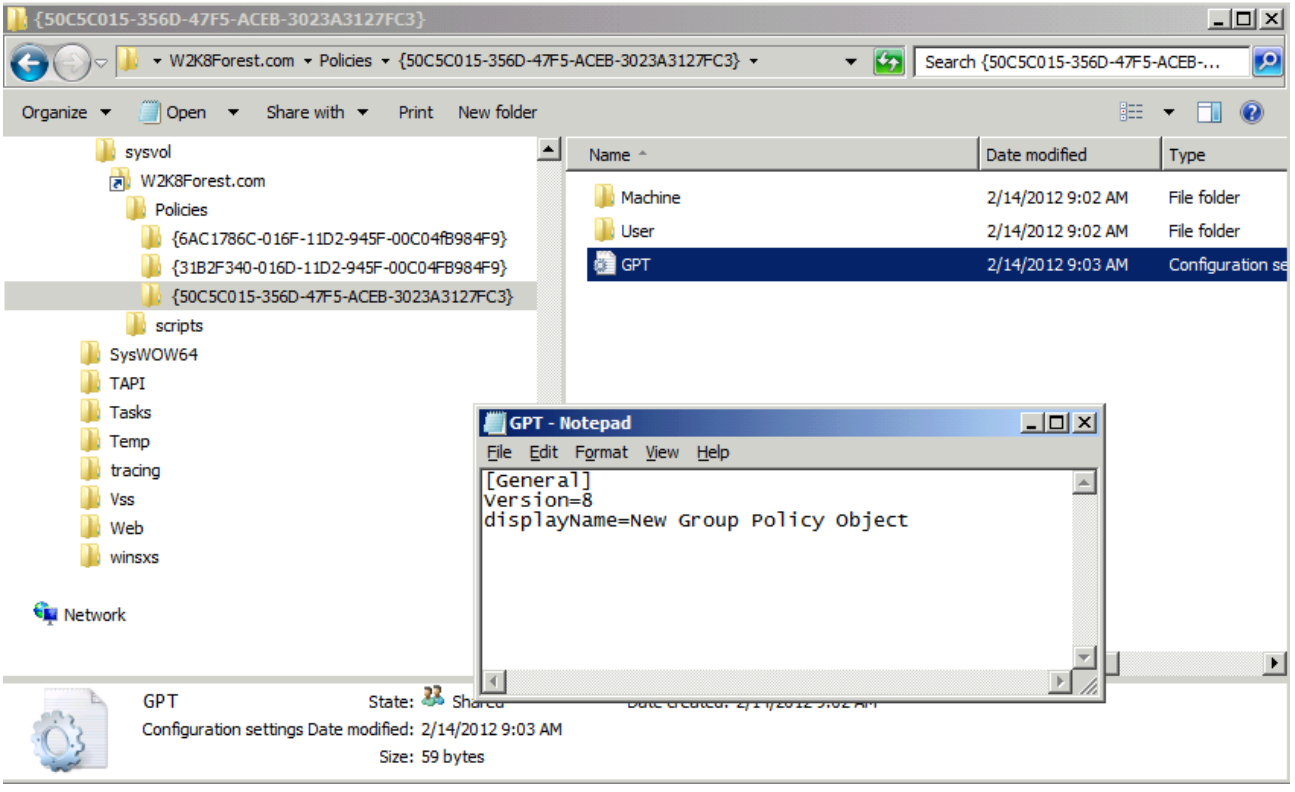


So now that you understand how to make these changes, what does the GPT look like once you've made them? Below is a series of screenshots to answer that question.

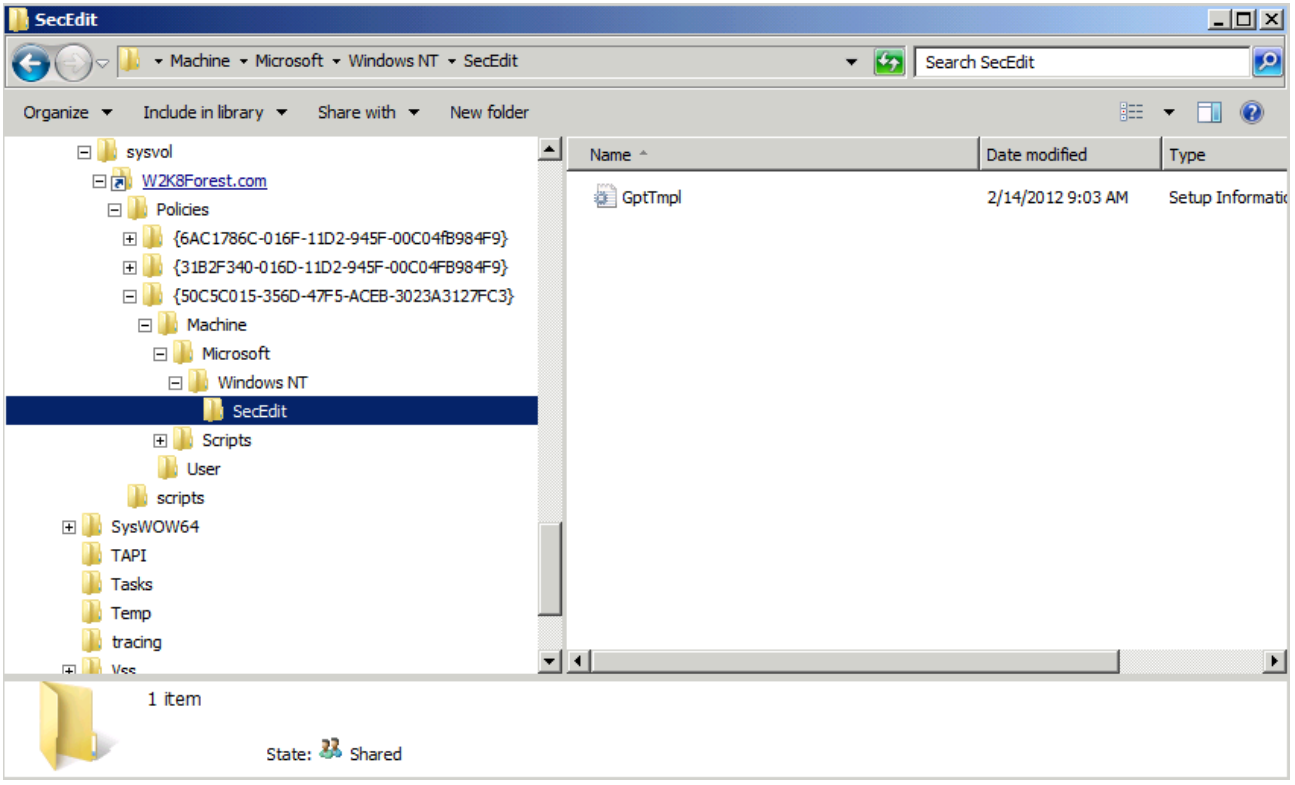
First, here is the file structure of the GPT, showing the GPO I've edited with its top level folders visible in the right-hand pane



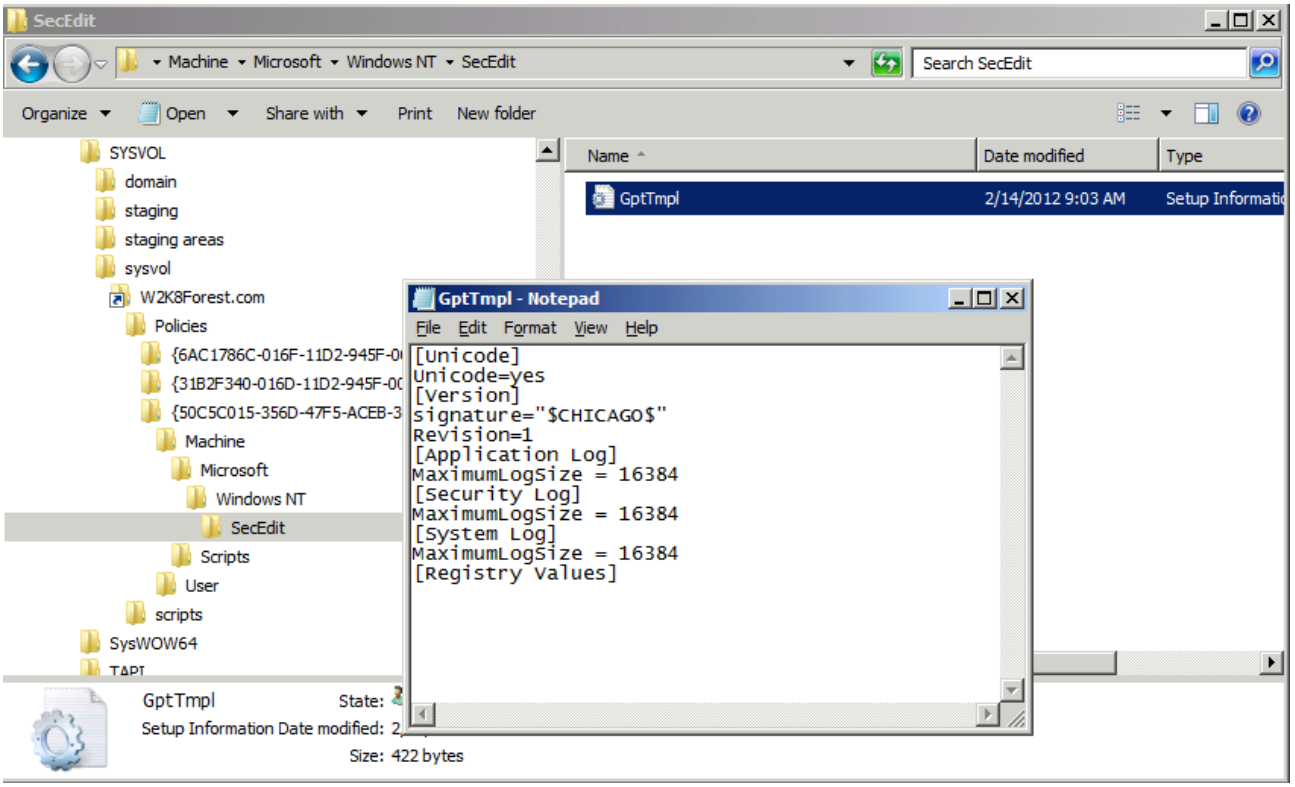
You'll notice the file called GPT (it's actually **GPT.INI**, though the screenshot hides the file extension). This file contains the configuration settings for this GPO, which includes its current version number (which is updated every time a change to the GPO is made) and the default GPO display name (which is the same for every GPO you create, so don't worry that it's not the name you gave it in the GPMC). Here is how that file looks (**NOTE: You can open GPT.INI with Notepad, but make sure you don't accidentally save it as a .txt file or it will impact your GPOs ability to do its job**)



To see the actual settings we've configured for this GPO, we need to expand the Machine folder (because this is a computer-side setting), which reveals the following:



You'll notice that there is a folder called **SecEdit**, which contains the security-specific settings of this GPO. The file within the SecEdit folder is **GptTmpl.inf**. It's this file that contains the specific information that your client needs to configure its settings. Because we've configured this GPO so that its Event Logs are set at the maximum size, we would expect that this file would contain information directing the client to make this change. By opening the file we can see that its contents do exactly as we would expect, as shown below (**NOTE: you can edit it with Notepad, but make sure you don't accidentally save it [or *GPT.INI*] as a .txt file after looking at it!**).



We can see from this picture that GptTmpl.inf has clear instructions for our client machine to set its Application, Security and System Event Logs to their maximum size.

As I said earlier, there can be numerous different settings in the GPT file structure depending on how you've configured your GPO. Other possible folders and files that might appear include:

- Scripts folder - This folder can contain information on which scripts to run, or may include the scripts themselves. The possible types of scripts include:
  - Startup/Shutdown: applies to Computers
  - Logon/Logoff: applies to Users
- Applications folder - if you've published or advertised software through a GPO, this folder will contain an advertisement file (.aas file extension) notifying clients of the software being made available
- Adm folder - Older GPO versions had Administrative Templates stored within the GPT on each Domain Controller. These templates were actually copied from client machines into the SYSVOL share of the Domain Controller. Starting with Vista, GPOs no longer do this (though if you edit a GPO with an pre-Vista OS, it will still behave this way). GPOs now leverage ADMX files that are stored in a Central Store on client machines (typically c:\windows\policydefinitions) instead of the GPT. But given that many older devices are still out there, you may see this folder in your GPT.
- Documents and Settings folder - this folder contains any Folder Redirectoin settings configured by the GPO.
- IEAK folder - this user-side folder contains settings related to Internet Explorer Maintenance.
- Registry.pol - this file contains the registry settings the GPO has been configured to apply. This file also contains any Software Restriction Policy settings that have been configured.

In part 2 of this series, we'll look at details of GPO processing, with an emphasis on Client-Side Extensions (CSEs). We'll also discuss how GPOs are replicated, and how a client knows it's getting the latest version of its GPO (including knowing whether the GPC and GPC are synchronized with each other).

- **Anonymous**
  January 01, 2003
  Good note, thanks for sharing :)

- **Anonymous**
  January 01, 2003
  No words...this is an excellent article!

- **Anonymous**
  August 21, 2013
  Thanks for sharing - simple explination for GPO

- **Anonymous**
  May 27, 2014
  awesome explaination...hard to find.

- **Anonymous**
  June 12, 2014
  good note, thank u for sharing

- **Anonymous**
  June 14, 2014
  Good explanation for easy self-practices...Thanks a lot!

- **Anonymous**
  July 15, 2014
  amazing one

- **Anonymous**
  August 15, 2014
  Useful post

- **Anonymous**
  August 20, 2014
  great post, thanks for sharing this

- **Anonymous**
  September 07, 2014
  amazing post

- **Anonymous**
  September 16, 2014

Thank You very much; you are appreciated!

- **Anonymous**
  October 21, 2014
  Excellent, very clearly, neatly explained. thank you so much.!

- **Anonymous**
  October 21, 2014
  Amazing.....Just what i needed!!!!

  Thanks a lot!!!!

- **Anonymous**
  November 24, 2014
  Nice one, Thanks.

- **Anonymous**
  December 17, 2014
  Good presentation for how to set up group plcy options thanks

- **Anonymous**
  January 14, 2015
  It's really helpful for administrators. Thanks a lot!!

- **Anonymous**
  January 19, 2015
  Excellent explanation of GPO Thanks a lot.

- **Anonymous**
  February 06, 2015
  Hello,

  thanks for explanation. Well done!

  one more thing, didnt you mean in the last sentence whether the GPC and GPT are sync?

  (including knowing whether the GPC and GPC are synchronized with each other).

- **Anonymous**
  April 01, 2015
  Very helpful post. Many thanks!

- **Anonymous**
  April 07, 2015
  It's good notes but we need short and sweet

- **Anonymous**
  May 06, 2015
  Thank you!!

- **Anonymous**
  May 06, 2015
  Thank you!!

- **Anonymous**
  May 20, 2015
  GPO made a chaotic impression to me until now. Since I read this post, everything is clear. - Thanks a lot!

- **Anonymous**
  May 20, 2015
  Trying to find an article to answer the question that if there is a setting in both the user's container in Active Directory users and computers AND there is also a group policy object that contains that setting, which one takes precedence? I am going to guess the GPO but am not sure (the setting is for the Remote Desktop Services idle session timeout - a bunch of users have these set on their user's object but I would like to set a policy at the domain level to override for everyone.

- **Anonymous**
  July 10, 2015
  Very clear and helpful... Request to post an article for group policy as SME preparation point of view

- **Anonymous**
  September 15, 2015
  can one recreate a missing gpt.ini?

- **Anonymous**
  September 15, 2015
  Quite helpful

- **Anonymous**
  October 08, 2015
  Its very nicely explained and easy to understand

- **Anonymous**
  November 08, 2015
  Great Work
