

# Re: Planning A Group Policy Deployment

---

*Source:*

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.group\\_policy/2007-07/msg00044.html](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.group_policy/2007-07/msg00044.html)

---

- *From:* "Roger Abell [MVP]" <mvpNoSpam@xxxxxxx>
  - *Date:* Wed, 4 Jul 2007 23:14:42 -0700
- 

"Edward" <Edward@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message  
[news:F762CAED-971F-430B-BFA9-5BF6AAD56230@xxxxxxxxxxxxxxxxxxxx](mailto:news:F762CAED-971F-430B-BFA9-5BF6AAD56230@xxxxxxxxxxxxxxxxxxxx)

"Roger Abell [MVP]" wrote:

I get the impression that you are so-to-speak being blinded by the trees and failing to view the forest from overlooks in the terrain.

I'd use a different metaphor. I have come to think of a complete Group Policy portfolio as the architectural plans for a multi-story building. There are myriad specs in such plans for things like floors, walls, engineering structures, windows, ventillation, electric, IP, etc. In order for the final design to make sense, and no matter what the final use of the building, there is still an underlying order to the development of the design. I am looking for that order, which you begin to hint at in your post, below.

I think we are on the same page.

At your stage of the game I am suggesting that you need to take an architectural view. The building architect knows that there are specific requirements (habitable, safe, space that is inviting, lighting needs for the different types of spaces, etc. etc.). You know, or could discover, what is done currently to provision computers, to customize user's environments, etc. and similarly you likely know business and regulatory needs. I was just suggesting that you should focus on these, and also prioritize them in order to attempt GP implementation of them in an appropriate sequence. Similarly, on the architectural vein, AD is (still) primarily a construct for admin/mgmt of the computing environment (i.e.

## Re: Planning A Group Policy Deployment

it has yet to be mainly a directory service). There is a great interplay as a result in the way computers and users are placed into the OU structure and the way the GP is applied to them. In a more ideal world one gets to factor policy settings so that they are stated once (in a single GPO) and this applies to the appropriate subset of the OU structure, compared to having the same policy value set in many different GPOs. So what I am attempting to indicate is that you sound like you are wanting a cookbook view of GP usage, and I am saying that how one uses GPOs depends on things beyond how GP works and beyond admin/mgmt objectives, especially the OU structuring.

So, first one needs to decide what aspects one wants to manage, and rank these as to their importance. Think functionally.

The more I ponder the question, the more it seems that the Security Guidelines for XP and Server should really be the first place to start (and yes, I am assuming a well developed Vision/Scope doc), regardless of the environment. These two docs seem to deal with foundational issues of network functionality and domain wide network access issues. Microsoft doesn't really take an emphatic position as to it's priority in the process. Here's my burning question for you: Is there any justification for starting elsewhere in a virgin domain?

Well, I am prejudiced when it comes to the guides you mention (as you may notice my name in the acknowledgements). But yes, I feel one can get some good ideas on how to use GP from the common scenarios Darren mentioned and on policy settings that are important for creating stable/safe deployments from those guides. However, notice that the guides deal mostly with the "security options" and make very little mention of settings in admin templates; the objective of the guides is to assist in hardening against an unknown, assumed hostile environment.

For examples: make machines accessible to only valid users, make machines silent on the network, have login scripts for users based on their user category, make sure all machines are using correct DNS servers, etc.

## Re: Planning A Group Policy Deployment

You present this as an alternative, but I think this may be an essential starting point in the absence of some extraordinary circumstance, which I obviously cannot even imagine. Do you agree? Above you actually cite four functional examples. Shouldn't each be treated one at a time, in terms of the design, test, rollout, evaluate cycle?

The examples I mentioned were just some things that came to mind, and did not intend to indicate priority. I was suggesting that you look at your environment (how computer/user provisioning is now done, the organizational objectives and business needs, etc.) and list out the different aspects that you hope to accomplish, and that you rank them in importance. Then look at how GP might be used (or not) to effect each. As you do that, you will start to see how some "fit" with the OU structure, and how some must get shoehorned into/onto it.

If you agree with everything above, I'm curious as to your preferred second and third areas of focus, absent unusual considerations.

My first area is to effect security and privacy; that is, to make sure I have done what is possible to make sure systems stay as they should be, are kept up-to-date, are resistant to penetration, are minimally visible on the network, etc. and allow only the intended users to have only the intended accesses.

My second area is to make the environment useful and convenient to its users. (short sentence, big task)

There are obviously some unstated prereqs for these, like a healthy network config and domain membership.

BTW, if you know of anyone who writes about process I'd be grateful.

Thank you.