

Re: Group Policy for hardened PCs

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.group_policy/2008-01/msg00283.html

- *From:* "Jeff Whitehead" <nospam.jeffwhitehead76@xxxxxxxxxxxxx>
 - *Date:* Thu, 24 Jan 2008 16:58:08 -0000
-

Hi Florian,

Thanks for your help here. We've managed to use the loopback processing mode as you suggest and it all seems to work.

I think your original solution using 2/3 different OUs was somewhat over complicated for us... but we've made it work using your basic concept.

For the benefit of others, we have left all our users and most of the machines in the root of the AD (i.e. in the Users and Computers containers respectively). These automatically pick up the default domain policy. I realise this is not strictly best practice, but as I said in my earlier mail, our structure is so simple, that creating lots of OUs really seems unnecessary.

I've created a single OU (DevelopmentPCs) and put ONLY the Development PCs in there (No users).

I've then created a policy assigned to this OU which has all the computer AND user settings AND made it 'Loopback', using 'Force' mode. [As a double-measure I've also told this OU not to inherit from above as I want this policy to override the domain policy].

Now when I log in as ANYBODY on the development PC [even a Domain Admin], the user settings for THAT PC apply.

If I log in as a developer on any other machine then the normal domain policy applies... I.e. their admin PCs are NOT locker down.

So, even though the Developers are admins on the local machines, because they log in as domain users, the GPO takes effect.

We've prevented them from running various applications, locked down IE to a single site etc.... and they can't override that.

Only if they log in as the local administrator (i.e. NOT a domain user) can they override any settings. As they don't have the local administrator password (only admin rights from their domain login) they will NOT be able to force any of our settings back to defaults.

This is just what we needed.

Re: Group Policy for hardened PCs

Thanks again for pointing me in the right direction!

Jeff.

"Florian Frommherz [MVP]" <florian@xx> wrote in message news:%23CRUFBeXIHA.4896@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Howdie Jeff!

Jeff Whitehead schrieb:

I've set up a new OU called Development and created a 'hardened' policy in there with lots of tweaks to both the Computer Settings and User Settings areas. [From what I can see, many of the IE policies we want... proxy settings etc, are in the User section rather than Computer]. I've then added the Development PC to this Development OU.

I'd go for a different approach. Create two three OUs: one OU for the developer users, one for the developer machines and one for the admin machines. In those OUs, you put the corresponding objects: user accounts into the developer users OU and so on.

Since most of your "hardening" policies are user configuration settings but you'd like to have it applied to the development machine, you'd configure them on the developer machines OU (under user configuration) and activate "Loopback processing mode". Loopback makes the machines apply the user configuration side of the policies that are in their scope (whereas they'd normally just ignore the user portion and only apply the computer side). Like that, all users, no matter who, will get the "hardened" settings you configure.

Loopback processing:

<http://www.frickelsoft.net/blog/?p=22>

http://www.microsoft.com/technet/prodtechnol/windows2000serv/reskit/distrib/dsec_pol_kcmb.msp?mfr=true

For those other two OUs you created, just make your settings in the corresponding configuration sides (user config for the developer users OU, computer settings for the admin machine OU).

- 1) To enable the specific user settings in this policy to be pushed onto the Development PC, I assume I will need to move the Developer's user accounts from the 'USers' container into the Development OU. Correct?

Yes and no. If there is a user configuration setting in a GP that is

Re: Group Policy for hardened PCs

linked to the Development PC and you move a user account into that OU, the Group Policy will apply. But it doesn't "stick" to the machine as the settings you made in that GP would apply to an admin pc if the user logged on there.

If so, then anything I put in the user settings, will then also apply to their Admin PC? Correct?

Correct.

We really need a config where the same user can log onto two different machines. One is locked down, and the other is not.
We thought of creating a second login for everybody, but that could become difficult to manage.

This is what loopback is for. Just have a look at that. No need for a second login.

2) Unfortunately, there is a 'bug' in one of the development tools that they use, which means users must be Administrators on their Development PCs.

If I make a user an administrator on their Development PC, does that mean that they can override all the Group Policy settings I apply? E.g. judging by some of the docs in the GPO editor, it looks as if they may be able to change IE settings etc if they are an admin?

Yes, they can – admins can do everything on their boxes. You can try to make it harder for them to get around your restrictions (like prohibiting the execution of cmd or regedit), but they basically can "undo" the changes – at least for the moment. Policy settings get re-enforced, "re-applied" every 90 minutes (+ a random offset of a max of 30 minutes) so their changes would be reverted back to what the policy says from time to time.

cheers,

Florian

--

Microsoft MVP – Windows Server – Group Policy.
eMail: [prename \[at\] frickelsoft \[dot\] net](mailto:prename@frickelsoft.net).
blog: <http://www.frickelsoft.net/blog>.

Re: Group Policy for hardened PCs