

Re: Need to filter domain admin from GPO

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.group_policy/2007-12/msg00140.html

- *From:* Meinolf Weber <meiweb(nospam)@gmx.de>
 - *Date:* Wed, 12 Dec 2007 06:55:04 +0000 (UTC)
-

Hello clarv02,

Ofc ourse you can deny the reading of the policy. But think always about the part that a deny is the highest blocking you set and if you forget that you have set a deny or you are not in and someone else have to search for errors, it will be really heavy to find it.

Peronally i would not set this kind of policy on the domain level, because everything there will also be applied for the servers. I prefer to use OU's for the different need's. Need's a bit more planning but i find it easier to manage.

Best regards

Meinolf Weber

Disclaimer: This posting is provided "AS IS" with no warranties, and confers no rights.

** Please do NOT email, only reply to Newsgroups

** HELP us help YOU!!! <http://www.dts-l.org/goodpost.htm>

On Dec 10, 10:55 pm, Meinolf Weber <meiweb(nospam)@gmx.de> wrote:

Hello clarv02,

Normally Block inheritance works fine. What GPO setting do you like to filter?

Best regards

Meinolf Weber

Disclaimer: This posting is provided "AS IS" with no warranties, and confers

no rights.

** Please do NOT email, only reply to Newsgroups

** HELP us help YOU!!! <http://www.dts-l.org/goodpost.htm>

On Dec 9, 11:59 am, "Matt" <mattd_em...@xxxxxxxxxxxx> wrote:

Re: Need to filter domain admin from GPO

I'm with Meiolf Weber on this one.

It's best practice to use a 2nd administrator account as your regular user anyway and leave the original admin account redundant only to be used as a fall-back. (According to the MS AD infrastrucute course your actually supposed to rename the original administrator for security purposes, maybe a bit of overkill but that's for a different debate!)

Sorry for digressing, yes I agree with creating a new user account (eg admin-clarv02) that is a member of the Enterprise Admins or Domain Admins group and pop it in a new OU with blocked inheritance. :-)

"Meinolf Weber"
<meiweb(nospam)@gmx.de> wrote in message

news:ff16fb6672bb38ca08a2707d6643@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Hello clarv02,

For the real domain administrator i would recommend:

- Rename the account
 - Set a strong long password
 - lock this password on safe place
 - DO NOTHING ELSE WITH IT
- CREATE a new account that is member of the domain admins group and move it to a new created OU e.g. ADMINISTRATORS and block the policy here.
- Best regards

Re: Need to filter domain admin from GPO

Meinolf Weber

Disclaimer: This posting is provided "AS IS" with no warranties, and

confers no rights.

** Please do NOT email, only reply to Newsgroups

** HELP us help

YOU!!!<http://www.dts-l.org/goodpost.htm>

I have a GPO that is at the domain level and I want to exclude the domain admin. It seems like the only options are:

* Security filtering (doesn't seem like the best idea)

* WMI filtering (can't seem to find any posts on how to make it filter user objects)

* Block inheritance (I would have to move the domain admin from Users to an OU)
I'm leaning

Re: Need to filter domain admin from GPO

toward the
last
solution.
But I'm
concerned
about
moving
the domain
admin
account.
The Users
container is
different
from
other
containers. I
guess it's a
system
container. It
doesn't
show up
like
the other
OUs in
GPMC.
And even if
I could
block
inheritance
to
that
container, I
don't want
to exclude
other users
that may be
in the
Users
container.
Is there any
downside to
moving the
domain
admin
account to a
different
container?
Or does
anyone
know of a
successful

Re: Need to filter domain admin from GPO

WMI filter
that I could
use?
(I do like
this option
but it seems
like no one
has been
able to
make it
work).

Thanks!–
Hide quoted
text –

– Show quoted text –

Thanks for the posts. I really should have thought of having a separate account for this. We have already renamed the administrator account with strong password. However, we do use it on a regular basis for admin tasks. That will change soon. I went ahead and created a special admin account for me to use and filtered the particular GPO using ACL deny. I couldn't seem to figure out how to block a single GPO at an OU level. Seems like I can block inheritance, but not from a specific GPO.

Anyway, thanks for the suggestions.– Hide quoted text –

– Show quoted text –

I have a GPO that specifies the IE Home Page. My understanding is that you can block inheritance, but it will apply to all GPOs above, unless they are enforced. Since I want to prevent a single GPO from applying to a group of people, I found it easiest to deny the read permission for that group.

Thanks,