

## Re: Domain Admins Group -- Trying to trim membership

---

*Source:* <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2006-06/msg00063.html>

---

- *From:* "Roger Abell [MVP]" <[mvpNoSpam@xxxxxxx](mailto:mvpNoSpam@xxxxxxx)>
  - *Date:* Tue, 20 Jun 2006 22:36:21 -0700
- 

roflol and thinking of the realities of the ages involved here <vbg>

"Joe Richards [MVP]" <[humorexpress@xxxxxxxxxxxxx](mailto:humorexpress@xxxxxxxxxxxxx)> wrote in message [news:e3cSxEMIGHA.4828@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:e3cSxEMIGHA.4828@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx)

Uncle Joe? LOL.

--

Joe Richards Microsoft MVP Windows Server Directory Services  
Author of O'Reilly Active Directory Third Edition  
[www.joeware.net](http://www.joeware.net)

---O'Reilly Active Directory Third Edition now available---

<http://www.joeware.net/win/ad3e.htm>

Steven L Umbach wrote:

Well hopefully Uncle Joe will reply also as he is one of the world experts on this topic. My two cents is that the risk of a misconfiguration or security breach rises almost exponentially with the number of domain admins you have so it makes sense to have a rather small group of only the most very trusted and competent people being domain admins.

In general almost all Active Directory management tasks can be delegated to a qualified regular domain user by managing AD object permissions. Such tasks could be creating and managing user and computers accounts, creating and managing groups, creating and managing OUs, and editing Group Policy. Of course there are things that only domain level administrators can do but those tasks such as managing privileged users/group, fsmos, global catalog servers, installing hardware/software on domain controllers, dcpromoting a server, installing a Certificate Authority, etc. usually are not done every day or even every week and

Re: Domain Admins Group -- Trying to trim membership

domain admins need something to do. An existing domain controller can also be dcpromoted to a regular server if you need non domain admins to service it. In a larger network I would think that domain controllers are only domain controllers running DNS and not also a print, file, DHCP/wins, or remote access server which make it easier to not want to allow other users to configure. There is a group called DNS administrators you can add users to if you need them to manage DNS and not be a domain level administrator. The white paper in the link below may be helpful. --- Steve

<http://www.microsoft.com/downloads/details.aspx?FamilyID=631747a3-79e1-48fa-9730-dae7c0a1c>

"Tom Glasser" <TomGlasser@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message  
<news:7E31AF20-C60D-49F6-ABE6-F910B0A6E584@xxxxxxxxxxxxxxxxxxxx>

I am being requested to analyze the current 15 – 20 members of the Domain Admins group with the goal of reducing membership in this group to an absolute minimum. But it seems at first blush that membership in this group is necessary to maintain various functionalities.

Is this a common problem in the Windows Server world? Anyone have similar experiences to share or any advice on attacking this issue?

Thanks!  
Tom