

# Re: Settle a Administrator's dispute

---

*Source:*

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active\\_directory/2006-08/msg01356](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2006-08/msg01356)

---

- *From:* "Jorge Silva" <jorgesilva\_pt@xxxxxxxxxxx>
  - *Date:* Fri, 4 Aug 2006 00:32:37 +0100
- 

Hi  
Inline

Our disagreeable admin says that if a Global Group is put into the Administrators Local Group on the DC but not in the Domain Admins Global Group, the users of the Global Group do not have the same permissions as the Administrator account -- particularly to add/modify/delete user/computer/group accounts in AD.  
Can you help settle this dispute.

- 1-By default the Administrator Account Belong to Global Group Domain Admins and the builtin/Administrators, Enterprise Admins,etc
- 2-By default members of the builtin/Administrators are the Enterprise Admins, Domain Admins and administrator.

Anyone who didn't say something like "Are you people crazy, there's no such thing as a 'local administrators' group on a domain controller

- Not sure that I agree with this... What "name" do we have to give at the user account (Administrator) used to logon in Active Directory Directory Services Restore Mode?
- Local admin? No?

and even if there were, adding people to it has nothing to do with local admin rights on workstations" is wrong.  
There is NO SUCH THING as a \*purely\* local group on a domain controller.  
Anyone who believes such a thing shouldn't be a domain admin. Sorry.

- Agree 100%, and more, a user added to builtin/Administrators has the rights to logon on the DC and make him of whatever group he/she wants.

Re: Settle a Administrator's dispute

I did test it by creating a user and putting him into the global group that's in the Administrators built in group and when I logged on with the user, I couldn't create/modify/delete users or modify distribution groups. I suspect the same for create/modify/delete computer and group accounts in AD as well.

This happens because members of the builtin/Administrators are not by default members of the local Administrators of the Clients Computers, Only The Domain Admins are (of course don't DO THIS).

To add the users (or some users, maybe your helpdesk staff) to the local Admins on client machines follow the Robert's instructions of configuring restricted groups policy.

—  
I hope that the information above helps you

Good Luck  
Jorge Silva  
MCSA  
Systems Administrator

"savvy95" <savvy95@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message [news:9A87EB67-724E-47DC-A47F-ACA8DCD87C3E@xxxxxxxxxxxxxxxxxxxx](mailto:news:9A87EB67-724E-47DC-A47F-ACA8DCD87C3E@xxxxxxxxxxxxxxxxxxxx)

I did test it by creating a user and putting him into the global group that's in the Administrators built in group and when I logged on with the user, I couldn't create/modify/delete users or modify distribution groups. I suspect the same for create/modify/delete computer and group accounts in AD as well.

I know who'll be buying the next round beer. I will.

Anyone want to join us ;)

"Robert Moir" wrote:

savvy95 wrote:

We have a dispute where one Admin disagrees with another 2 regarding the Administrators Local Group ON THE DOMAIN CONTROLLER. We are not talking about the group on the workstation.

## Re: Settle a Administrator's dispute

I'd like confirmation that I'm correct.

Our disagreeable admin says that if a Global Group is put into the Administrators Local Group on the DC but not in the Domain Admins Global Group, the users of the Global Group do not have the same permissions as the Administrator account -- particularly to add/modify/delete user/computer/group accounts in AD.

Can you help settle this dispute.

Sure. That bit is easy.

Anyone who didn't say something like "Are you people crazy, there's no such thing as a 'local administrators' group on a domain controller, and even if there were, adding people to it has nothing to do with local admin rights on workstations" is wrong.

There is NO SUCH THING as a \*purely\* local group on a domain controller. Anyone who believes such a thing shouldn't be a domain admin. Sorry.

If you've been adding domain users to the built in 'Administrators' group then you've essentially made all those users administrators of your domain controllers (including, by default, active directory). Test one and see.

The original problem was to give domain user accounts local administrator rights.

Oh. In that case why not try something like this:

<http://www.microsoft.com/technet/scriptcenter/resources/qanda/sept05/hey0923.mspix>

Or with a restricted group in group policy. To create a Restricted Group do something like this:

- Edit Group Policy.
- Choose Computer Configuration, Windows Settings, Security Settings, Restricted Groups.
- Right-click on Restricted Groups and select Add Group.
- Click Browse.
- Type the name of the group and click OK.
- Click OK again on the Add Group dialog box.
- On the top section labeled Members of This Group click the Add button.
- Click Browse.
- Type in or browse for the desired users or groups that should be

Re: Settle a Administrator's dispute

members  
of the new local Restricted Group. After adding members to the group.  
– Click OK to finish and close the dialog box.

By the way, giving domain users administrative rights on their  
workstations is a very bad idea but then it sounds like they're already  
domain admins so I don't suppose it makes much difference now.

--  
--

Rob Moir, Microsoft MVP for Security  
Blog Site – <http://www.robertmoir.com>  
Virtual PC 2004 FAQ –  
<http://www.robertmoir.co.uk/win/VirtualPC2004FAQ.html>  
I'm always surprised at "professionals" who STILL have to be asked:  
"Have you checked (event viewer / syslog)".