

Re: Unable to add domain user or groups

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2007-01/msg00142.html

- *From:* "Kerry Brown" <kerry@xxxxxxxxxxxxxxxxxxxxxxx*a*m>
 - *Date:* Mon, 8 Jan 2007 08:10:38 -0800
-

Check the DNS settings on an affected workstation. It sounds like they are not using a domain DNS server.

—

Kerry Brown
Microsoft MVP – Shell/User
<http://www.vistahelp.ca>

"RichardH" <RichardH@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
<news:25BF3281-2387-4239-9902-86C6AACE3DBE@xxxxxxxxxxxxxxxxxxxx>

Thank you for the advice; however, there is a very real problem here. The problem is much more severe than I thought. We are unable to add domain users to local folder permissions, groups, etc. As soon as we check the name, we get a message saying that windows cannot process the object... access is denied. We can add local users to directory permissions but we cannot add any domain user or group. There doesn't seem to be an audit log of this denial.

There is not a domain group policy causing this problem and it is now affecting all computers in the domain except for a few that have been completed in the past few weeks. It is like the administrators lose their rights after a short period of time. Administrators can log in normally, they can get to all domain resources, they can even change local settings. However, administrators cannot perform windows update except if logged in as the local administrator and cannot add domain users to local resources etc.

"Lanwench [MVP – Exchange]" wrote:

In <news:AE98D623-187F-4BC2-A970-C9A77C94F808@xxxxxxxxxxxxxxxx>,
RichardH <RichardH@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> typed:
> I have tried adding users with both a domain admin account as well as
> logged in locally as an administrator and then supplying the domain
> information when asked (domain\username and password).
>

Re: Unable to add domain user or groups

- > We have done this without any problems in the past and some machines
- > accept the additions without any problems.
- >
- > After typing the group or username of the domain object I am wanting
- > to add and click "check name", I get a message stating that windows
- > cannot process the object... Access is denied. For example, if I
- > were to enter "tjones" and then click check name... it would respond
- > "Windows cannot process the object Jones, Thomas... Access is
- > denied."

I have to echo Jesper's comments – this is generally a Really Bad Idea. If you have software written by lazy developers who don't understand secure multiuser operating systems, you can usually force them to play nice by figuring out which file system & registry places the app expects to write to – try filemon & regmon (google) for help.

That said, since you've got AD, why do this at the workstation anyway? You have a couple of better options – restricted groups, or even a computer startup script. I like to create two AD groups: LocalAdmin and LocalPowerUser. I add them to the respective workstation groups via startup script. I can then add the domain users to the AD groups and remove them at will, from one location....but I don't like to have users run as anything other than users, for daily driving.

You might post in a GP group if you need more information on this.

- >
- > "Jesper" wrote:
- >
- >> First, why would you want users to be full local administrators? It
- >> is a really bad idea.
- >>
- >> Second, at what point do you get the access denied? If you are
- >> logging on with a non-domain account you would get it trying to
- >> access the user list on the domain. More likely though is that you
- >> are logged on with a non-administrative account that does not have
- >> the right to modify the Administrators group.
- >>
- >> "RichardH" wrote:
- >>
- >>> When I attempt to add a domain user or group to the local
- >>> administrator group, "Access is denied".
- >>>
- >>> I have tried removing the computer from the domain and adding it
- >>> back.
- >>>
- >>> We are able to add users and groups from cmd line, but the settings
- >>> don't actually apply. Users still do not have full administrative
- >>> priviledges.
- >>>
- >>> We are running Windows XP Professional SP2 on our clients and

Re: Unable to add domain user or groups

>>> Windows Server 2003 on our domain controller.