

Re: Adding local users from domain as local PC admin(?)

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2006-02/msg02092

- *From:* "kj" <kj@xxxxxxxxxxx>
 - *Date:* Sun, 26 Feb 2006 21:16:55 -0700
-

It sure would be helpful to have a restricted group option to either "add" or replace" wouldn't it?

Too many cusrmgr uses to forget about it.

--

/kj

"Cary Shultz" <cwshultz@xxxxxxx> wrote in message
<news:%23yfUNehOGHA.3856@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

Paul,

I agree that if you have to do this on one machine – or on a couple – then the script or Computer Management is a good way to do it. You can do it remotely instead of having to sit at the system in question.

I, also, agree that if you have a lot of computers where this needs to be done then –EITHER– Restricted Groups –OR– a script would be a good way to do things.

I think that (and please correct me where I am wrong) your problem with Restricted Groups is that the default behavior is to purge all members of 'local group in question' and replace it with 'your group of choice'. This can become a problem, especially if the person using this does not know about this behavior and forgets to add the Domain Admins group. This does indeed create a problem...

Additionally, if one does not follow the MSKB article to a tee, specifically after Step 3 (IIRC), and tries to do this on a Domain Controller that person is going to have one heck of a time!

But, there is a fix to the default behavior. This does require that the fix is applied to all systems in the environment (might be a bigger problem than it is worth) and you do need to make sure that the correct patch is applied to the correct system (meaning, that the WIN2000 patch is applied only to WIN2000 systems and that the WINXP patch is applied only to WINXP systems).

Re: Adding local users from domain as local PC admin(?)

In some environments I rather like the default behavior. Too many times I have seen someone grated 'local Administrator' group membership and the "dam has been breeched".

I also agree that if Restricted Groups is used too much that it is a bad thing. But, with all things, moderation is the order of the day!

And, I am glad that you like cusrmgr. Everyone seems to forget about this tool! Or, just not know about it!

—
Cary W. Shultz
Roanoke, VA 24012

"Paul Williams [MVP]" <ptw2001@xxxxxxxxxxxx> wrote in message
news:1140698768.2738@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

For a one off operation, COMPMGMT.MSC or a script should be used. For global changes, restricted groups can be used but tends to do more harm than

good. Remember, restricted groups is designed to enforce group memberships.

Personally, I find a script (startup or run as an admin) the best way of doing this as you can log this information and create a rollback mechanism.

Another way, of which I have only just learnt, is CUSRMGR.EXE.

You must also consider what you are doing and why. For specific users, this

is tedious and wrong. REGMON, FILEMON, and the Application Compatibility

Toolkit are what is needed in this scenario.

I've seen too many problems caused by widespread use of restricted groups.

It is a great feature, but if you have customised local groups on an ad-hoc

computer basis, it causes all manner of problems (followed by grief).

—
Paul Williams
Microsoft MVP – Windows Server – Directory Services
<http://www.msresource.net> | <http://forums.msresource.net>

Re: Adding local users from domain as local PC admin(?)