

Re: Group Policy setting for restricting creation of local user accounts

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.group_policy/2006-10/msg00024.html

- *From:* "KenB" <kbrussel@xxxxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 3 Oct 2006 09:12:41 -0400
-

This is definitely a training issue. Domain Admin rights should not be handed out haphazardly. You wouldn't make a 5 year old president of the US, right? Why? Because they have no idea what they're doing.

If these so-called 'admins' need rights within the domain, there are ways to grant them rights without giving them too much power. i.e. the Delegation of Control Wizard in A/D, and various groups on workstations.

Ken

"Roger Abell [MVP]" <mvpNoSpam@xxxxxxx> wrote in message <news:u4v2bLr5GHA.508@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

Well, you have now significantly changed the scenario. There is really no way to prohibit a Domain Admin from doing what they want to do. You can make it more difficult, but your ultimately cannot do it.

For example, if DA was not in each machine's local Administrators group, then they could not do anything to those machines – until they forced their account to again become member in Administrators on those machines (which they could do).

You probably need to address your issue either by not having as DAs those that you do not trust to needed extent, and/or by having clearly stated limits on acceptable/unacceptable actions for DA power usage with expectation that they will conform to the limits.

"B.E. Jorgenson" <jorgenson.b@xxxxxxxx> wrote in message <news:1159804569.016570.299160@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

Here's the problem.... I have domain administrators that I do not want creating local users on computers. Would I have to create a restricted group that mimics domain admins rights minus the right to create local users?

Re: Group Policy setting for restricting creation of local user accounts

Roger Abell [MVP] wrote:

"B.E. Jorgenson" <jorgenson.b@xxxxxxxx> wrote in message
news:1159560514.691170.269170@xx

Right, but I am looking for a group policy, security template, or local security policy.

You could use a restricted group definition in a GPO applied at an OU level (not to DC OU or to Domain) that carries definition for Administrators naming only what you want included in them all. It is often convenient for that GPO to also had a rename policy set renaming the built-in Administrator

KenB wrote:

Restricting the users to non-administrator access will prevent them from being able to create accounts on the computers.

Ken

"B.E. Jorgenson"
<jorgenson.b@xxxxxxxx>
wrote in message
news:1159380582.077768.320930@xx

Is there a way through group policy to restrict any user from creating

Re: Group Policy setting for restricting creation of local user accounts

local
computer
user
accounts
when the
computer is
joined to
the
domain?
This has
nothing to
do with
logon
locally but
actually
creating a
local
user
account.

Thanks,
Brian