

# Re: Preventing Users from removing their PC from the Domain

---

*Source:* <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2006-06/msg00069.html>

---

- *From:* "Roger Abell [MVP]" <mvpNoSpam@xxxxxxx>
  - *Date:* Sun, 25 Jun 2006 09:26:34 -0700
- 

Entering, or not, valid domain credentials at the domain prompt during a disjoin in my experience only impacts whether the computer object is removed, or not.

But I agree, local admin should be required in either event.

"Steven L Umbach" <n9rou@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message [news:%238bvG4BmGHA.2056@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:%238bvG4BmGHA.2056@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)

I have seen the behavior where you don't need to enter valid credentials if you are logged on as a local administrator. Whenever I have not been logged on as a user that is not in the local administrators group either explicitly or by group membership I can not even access the change name or network ID settings as they are grayed out and a message shows that only a local administrator can do such. I would double check that you are not logged on as a user that is also a local administrator whether that be a domain account or a local account. I would try it again but before hand it would help if you could post in a reply the results for the whoami /groups command for the logged on user that can remove the computer from the domain and the command net localgroup administrators. Whoami can be downloaded from Microsoft and I believe it is a RK tool. --- Steve

<rndinit9@xxxxxxxx> wrote in message [news:1151212284.901984.169050@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:1151212284.901984.169050@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)

thank you Steven, however I logged on as a non local administrator. To be more specific a user.

The user does not have any privlidges what so ever. They cannot install or uninstall software, but im willing to bet that even the guest account (disabled by default) would be able to remove the PC from the domain.

The funny thing is, when it prompts the user for a user name or password, if you leave those fields blank and hit ok, it will work. And the PC is removed from the domain. Would appreciate more replies.

Steven L Umbach wrote:

Re: Preventing Users from removing their PC from the Domain

A user needs to be a local administrator in order to remove their computer from the domain. So the obvious answer is to not allow the user to be a local administrator and look at ways for the user to function as needed without being a local administrator. I know that may not always be possible. There is no magic bullet to prevent local administrators from removing their computer from the domain as local administrators by definition and design are all powerful on their computer. About the best you can do is to have a strict user policy that users sign and understand and that removing computers from the domain is prohibited. You can also use Group Policy to try and hide access to ways a user would use to remove their computer from the domain if it does not interfere with their needed access to the operating system. Group Policy can be used to hide or remove access to Control Panel applets such as System which is probably what most users use. That will not work however for skilled and determined users.

---

Steve

<rndinit9@xxxxxxxx> wrote in message  
[news:1151146580.725415.255000@xx](mailto:news:1151146580.725415.255000@xx)

rndinit9@xxxxxxxx wrote:

Currently users are able to remove their PC's from the domain w/o being prompted for a DomainAdmin

Re: Preventing Users from removing their PC from the Domain

username/pass. This is  
becomming a  
problem.  
How can I set it that in order  
for a PC to be removed from  
the  
domain,  
that a domain admin  
username & password must  
be entered.

Your help is appreciated.

To add some info: The DC is Windows 2000