

# Re: Problem managing accounts in protected groups

---

*Source:*

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active\\_directory/2008-09/msg01499](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2008-09/msg01499)

---

- *From:* Steve <[Steve@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:Steve@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Mon, 29 Sep 2008 10:14:03 -0700
- 

Thank you very much for the information.  
I will look into incorporating it.

--

Technical Support is usually neither.

"Meinolf Weber" wrote:

Hello Steve,

For your admins, you should think about using this way. Most common praxis as far as i know. For you administrator accounts create an own OU directly under the domain name and place there the domain admin accounts without any restrictions through policies or whatever.

And create for them a normal domain user account for the daily work with normal restrictions like any other user. If they have to do admin tasks, they can choose RUN AS option for that and use the domain administrator account. If now the account under the Administrators OU is locked another one from that OU can easily unlock them without any problem, because they all are domain admins in that OU.

Best regards

Meinolf Weber

Disclaimer: This posting is provided "AS IS" with no warranties, and confers no rights.

\*\* Please do NOT email, only reply to Newsgroups

\*\* HELP us help YOU!!! [http://www.blakjak.demon.co.uk/mul\\_crss.htm](http://www.blakjak.demon.co.uk/mul_crss.htm)

Meinolf,

I know that the request seems strange, but the members of the new group are not just any users.

Re: Problem managing accounts in protected groups

We are a small company. we have two domain admins: the IT Manager and the Network Admin. It is not uncommon for only one of us to be in the building.  
If one of us is locked out without the other here, it is a big hassle because not only can we not do OUR work, we can't help anyone else either. The others that would be in the Account Management group would be the CFO/CIO and our System Support person (who the member of Backup Operators). We would like for one of them to be able to unlock one of the Admins if they become locked when the other isn't there.  
I hope that makes things a little clearer.  
"Meinolf Weber" wrote:

Hello Steve,

If your normal domain users that manage accounts are aible to manage also the higher level administrators, you kick yourself in.....  
Never heard about that someone will give more security permissions to users then to the admins.

I think you have realized that the account management group is able to reset a domain admins password and work themself as admin if your configuration gets working completely?

What's the reason for this kind of configuration?

Best regards

Meinolf Weber

Disclaimer: This posting is provided "AS IS" with no warranties, and confers no rights.

\*\* Please do NOT email, only reply to Newsgroups

\*\* HELP us help YOU!!!

[http://www.blakjak.demon.co.uk/mul\\_crss.htm](http://www.blakjak.demon.co.uk/mul_crss.htm)

Before I ask my question, here is our basic setup:

## Re: Problem managing accounts in protected groups

We have a single Windows 2003 Domain. Within the domain there are two OUs that contain users. OU A has users who DO NOT have desktop restrictions through GPOs and OU B is for users who DO HAVE some desktop restrictions. We have created a new group called Account Management. This group contains users in both OUs and should have permission to unlock accounts and reset passwords. The permissions for this group have been applied to OU B and it all works perfectly. The permissions for this group have also been applied to OU A.

Here is the problem. Most members of OU A are either members of Domain Admins or Backup Operators. Even after setting the permissions on the AdminSDHolder container and having those permissions propagate to the protected accounts, the Account Management group still cannot manage lockouts or passwords for the users in the protected groups. Users in OU A who are not in protected groups can be managed properly. I know that there is a way to remove certain groups from being protected, but I do not have permission to do that. How can I get this group to be able to manage members of the protected groups? I would appreciate suggestions for other things to try, or pointers in the right direction. Thank you.

Re: Problem managing accounts in protected groups