

# Re: Delegation – Password Reset – Access Denied

---

*Source:*

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active\\_directory/2006-12/msg01299](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2006-12/msg01299)

---

- *From:* TimJM <[TimJM@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:TimJM@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Mon, 18 Dec 2006 11:07:00 -0800
- 

No the permissions are not what I expected. The user can change passwords but not reset the password. After looking at this I removed the group from the OU security and ran the Delegation Wizard again. Same results.

Here is the structure of the OU's

Building – Computers  
Groups  
User

Delegation is set at the building level and inherited to the others. The Group (BldgAdmins) that I am setting up as a delegate exists in another domain and is a global group.

If I create a new account in the Users OU as a user in the BldgAdmins group the user can then reset the password. If I try to reset an existing account I get the "Access Denied error". I then added an account as a Domain admin, to test if the BldgAdmins User can reset this new users password. This was successful.

After discovering this I reviewed the security settings on some of the User Accounts in the OU and found that the BldgAdmins group was not listed. I then added the BldgAdmins group to an existing users account and set this group for Full Control the a BldgAdmin User can then reset the password on that account.

It looks as though the delegate group is not getting inherited to the existing accounts. I then reviewed some of the existing accounts and discovered that these user accounts were not inheriting permissions.

After discovering this I searched the KB and found this 306398 article. I remebered reading this before and because it looked like it was only for Win2K and I'm running W2k3R2. The enviroment I'm woking is is a pilot for a roll out planned early next year. The person who started this pilot had placed a logon script in the default domain GPO that added the domain users group into the local Administrators Group. Why I don't know. But this was also adding the domain users into the Administrators group on the domain controllers which is not a Local Group on those machines. So needless to say

Re: Delegation – Password Reset – Access Denied

every user on the domain was being made an admin!!!!. I removed this script to stop this behavior. It looks like this might have caused this problem.

Do you know of an easy way to reset all of these user and group accounts to have inheritance turned on?

Thanks,

TimJM

"Paul Bergson [MVP-DS]" wrote:

You attempt to see if the permissions are being applied as you expected.

Open up a user's properties and select the security tab, click on advanced, select the effective permissions tab, click on select and enter a user in and select ok.

What permissions are shown in the window? Are they what you expected?

--

Paul Bergson  
MVP – Directory Services  
MCT, MCSE, MCSA, Security+, BS CSci  
2003, 2000 (Early Achiever), NT

<http://www.pbbergs.com>

Please no e-mails, any questions should be posted in the NewsGroup  
This posting is provided "AS IS" with no warranties, and confers no rights.

"TimJM" <TimJM@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message  
<news:33231D18-CE57-4A1C-9D28-5C125DD50A67@xxxxxxxxxxxxxxxxxxxx>

I understand that and that is what I'm trying to avoid. I feel I have followed the correct procedure to delegate a group to manage a branch of the AD. This group is closed to the needs of those users and will be the 1st line of help. I want them to create users and security groups, place users in those groups and reset passwords when needed.

The issue is it everything looks like it is setup properly, but when a user in this group tries to reset a password, they get an access denied message. I have reviewed permissions and they look correct. The group has Full control

Re: Delegation – Password Reset – Access Denied

on both group and User objects. These permissions are inherited from the OU above.

To me it looks like something else is preventing the user in this group from resetting passwords, and that is what I'm looking for direction on as to where else beside the KB to look for this answer?

TimJM

"Paul Bergson [MVP–DS]" wrote:

Don't ever place a user in any of the Administrative groups unless you are willing to provide them administrative privileges.

--

Paul Bergson  
MVP – Directory Services  
MCT, MCSE, MCSA, Security+, BS CSci  
2003, 2000 (Early Achiever), NT

<http://www.pbbergs.com>

Please no e-mails, any questions should be posted in the NewsGroup  
This posting is provided "AS IS" with no warranties, and confers no rights.

"TimJM" <TimJM@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message <news:F6B45477-9F43-40F7-BA6F-E328192739D3@xxxxxxxxxxxxxxxxxxxx>

I have setup a group as delegate to an OU.  
This group has Create, delete, Manage User accounts & Groups, Reset user password, read all user info, and Modify Group Membership.

I have setup a custom TaskPad for them to use. When a user in this group tries to Reset a Users Password the get an Access Denied error. I read in

Re: Delegation – Password Reset – Access Denied

another post on this group that that group  
needs to be in the  
Administrators  
group. Doesn't this defeat the whole purpose  
of delegating control?

When I do add this group into the Admins  
Group a user of that group can  
Reset Passwords. Am I missing something?

TimJM