

# AD Delegation problems

---

*Source:*

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active\\_directory/2008-07/msg00872](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2008-07/msg00872)

---

- *From:* "Randy Jackson" <[rjackson@xxxxxxxxxxxxxxxx](mailto:rjackson@xxxxxxxxxxxxxxxx)>
  - *Date:* Mon, 21 Jul 2008 12:11:25 -0400
- 

I used the AD delegation wizard to give a security group permission to create/modify/delete user objects and groups for a user and group OU. This OU has several sub OU's.

After using the wizard I went back and switched my ADUC to advanced view and modified the security list to prevent this group from deleting users and creating/deleting groups by using the explicit DENY permission. I checked the effective permission on the parent and child OU's for a user in the security group and both show that they have the rights to create users but not be able to delete them or create or delete groups.

I then have this user open ADUC and try and create a user and delete a user from the parent OU. They are able to create but not delete a user, even a user they created. They are also unable to create or delete groups, which is great. However, in all of the child OU's, this user is able to delete user objects, but the funny thing is they can not create groups.

Why is the delete user security setting not propogating down to the child OU's? I went in and select for the "Deny delete user objects" to apply to this container and all child objects, however that still does not work. I've checked the "Delete" and "Delete subtree" options as well and set those to Deny, still no luck.

Any one have any idea on how I can give this group the ability to create users but to not be able to delete any object?

Also, I've given them the ability to create all child objects and denied them the ability to delete any child object. I would like them to be able to create a new user account and setup the Exchange mailbox with the user, however even with being able to create all child objects on a user account, they still can not select the store to place the user in when creating a new account.

Thanks in advance for your help.

.