

# Re: Delgation of control above the OU grants additional rights which provide Full Control for the user

**Source:**

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active\\_directory/2004-09/0827.html](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2004-09/0827.html)

---

**From:** Joe Richards [MVP] (*humorexpress\_at\_hotmail.com*)

**Date:** 09/11/04

Date: Sat, 11 Sep 2004 10:36:09 -0400

Just in case the OP needs more than one person saying this. I completely concur with Steven. You can't do it. The builtin creator/owner functionality won't allow it.

In this case you would be best off setting up a web site to proxy the work. The NewAdmin goes to this web site and requests the change. The web site does it with its own userid on behalf of the newadmin, that way the ID the website runs under owns the new ou's or better yet it reassings the ownership to admins.

joe

--

Joe Richards Microsoft MVP Windows Server Directory Services  
www.joeware.net

Steven L Umbach wrote:

> You can't do what you want. When you allow a user to create an OU, that user is the  
> owner of that OU and hence can change permissions on the OU. Delegation of authority  
> is nothing more than assigning permissions. You may want to allow only domain admins  
> to create OU's or make sure that person you want to create OU's is someone who is  
> competent and you can trust. --- Steve

>  
>

> "Vlad" <tokov\_00@yahoo.com> wrote in message  
> news:912c09b.0409060754.33525b0e@posting.google.com...

>

>>Hello All,

>>

>>Please help me to accomplish the solution for the Scenario:

>>

>>Windows 2003 domain: mydomain.com

>>NewAdmin is a member of CN=Users,CN=mydomain,CN=com. NewAdmin is not a  
>>member of any Administrator groups.

>>BadUser is a member of CN=Users,CN=mydomain,CN=com. BadUser is not a  
>>member of any Administrator groups.

>>There is an OU: OU=MyOU,CN=mydomain,CN=com

>>

>>WE WANT:

>>- to delegate the ability to create, rename and delete Organizational

>>Units to NewAdmin. These OUs should be sub-OUs of the

Re: Delgation of control above the OU grants additional rights which provide Full Control for the user

public.windows.server.active\_directory: Re: Delgation of control above the OU grants additional rights which provide Full C

```
>>OU=MyOU,CN=mydomain,CN=com.
>>- to delegate the ability to create, rename and delete Computers in
>>the created OUs.
>>
>>WE DO NOT WANT:
>>- NewAdmin to be able to delegate any permissions to the sub-OUs which
>>were created by the NewAdmin in the OU=MyOU,CN=mydomain,CN=com.
>>
>>UNWANTED RESULTS OF THE SCENARIO:
>>NewAdmin creates OU: OU=NewOU,OU=MyOU,CN=mydomain,CN=com
>>NewAdmin delegates Full Control to BadUser over
>>OU=NewOU,OU=MyOU,CN=mydomain,CN=com.
>>
>>TRIED, BUT DID NOT HELP:
>>- Tried to delegate the control with the help of the Delegation of
>>Control Wizard.
>>- Tried to edit the Special Permissions on the
>>OU=MyOU,CN=mydomain,CN=com with and without "Allow inheritable
>>permissions from the parent to propagate to this object and all child
>>objects" checked.
>>- Tried to edit the Special Permissions on the
>>OU=MyOU,CN=mydomain,CN=com as
>>First set Full Control to Deny and then allowed only
>>List Contents
>>Read All Properties
>>Read Permissions
>>Create Computer Object
>>Delete Computer Object
>>Create Organizational Unit Object
>>Delete Organizational Unit Object
>>for the "Apply onto:
>>This object and all child objects
>>Organizational Unit objects"
>>
>>POSSIBLE REASON OF FAILURE:
>>Wrong settings in the
>>- Permissions
>>- Apply onto
>>- Object Name
>>- Inheritance
>>
>>Thank you for your help.
>>Vlad
>
>
>
```

Re: Delgation of control above the OU grants additional rights which provide Full Control for the use