

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

Source:

http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.setup_deployment/2004-09/0048.html

From: Steven L Umbach (*n9rou_at_n0-spam-for-me-comcast.net*)

Date: 09/06/04

Date: Mon, 06 Sep 2004 19:42:09 GMT

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 OUs or make sure that person you want to create OUs 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

> 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

ft.public.win2000.setup_deployment: Re: Delgation of control above the OU grants additional rights which provide Full Con

- > *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