

Re: Custom rights

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2005-07/0242.html>

From: Miha Pihler [MVP] (*mihap-news_at_atlantis.si*)

Date: 07/16/05

Date: Sat, 16 Jul 2005 21:50:22 +0200

Hi,

Try giving user who is adding account View Only Exchange Administrator permission. You should do this using a wizard in Exchange (e.g. on Exchange Organization or some other level)...

I hope this helps,

--

Mike

Microsoft MVP - Windows Security

"GraXi" <GraXi@discussions.microsoft.com> wrote in message
news:31E32CB0-11E8-4D92-8A3E-847A4E801CD7@microsoft.com...

> Steven,

>

> This was also very useful to me. However, when my test .tech user tries to
> create an account he goes thru the process fine until I arrive to the

> "Create

> an Exchange mailbox" screen.

>

> I can see the "Server" but I can't see the "Mailbox store". What do I need
> to add/modify in order to get this done.

>

> Thanks

> GraXi

>

> "Steven L Umbach" wrote:

>

>> OK. Try this.

>>

>> By default any user can log onto a server other than domain controller.

>> To

>> allow then to logon to a domain controller give them the logon locally

>> user

>> right in Domain Controller Security Policy. Note the user possibly could

>> manage what he needs from another computer through mmc snapins.

>>

>> To add computers to the domain go to AD Users and Computers. Select view

>> advanced features. Then select the domain, right click and select

>> delegate

>> control. The wizard will start. Add your user/group and select add

>> computers

>> to the domain.

>>

>> To add users to the domain go to the domain

Re: Custom rights

microsoft.public.win2000.security: Re: Custom rights

```
>> container/properties/security/advanced/add - select your group/select
>> "create user objects" and apply. This allows them to create but not
>> delete
>> users.
>>
>> To add users to a specific groups. In the properties of the groups go to
>> security/advanced/add - select your group/select properties at the top
>> [instead of object]/select "write members" and apply. Of course this will
>> not work on privileged groups such as administrators.
>>
>> To reset password for non privileged user accounts. Go to
>> domain/properties/security/advanced/add - select your users group/select
>> "apply onto:" user objects/select reset password and apply. By default
>> privileged accounts do not inherit permissions to exempt them from
>> delegation. If you have a user in a privileged group and you remove that
>> user, you will have to manually configure permissions on that user object
>> or
>> select "allow inheritable permissions to propagate from parent".
>>
>> The above should allow a regular user account in the domain to do what
>> you
>> want. A regular user can not install most software. Personally I would
>> not
>> want any regular user to logon to a domain controller but instead they
>> can
>> use mmc snapins to mange what they need which will prevent them from
>> having
>> access and installing anyhting on the domain controller. I would also
>> suggest you consider giving the user/group those powers [except add
>> computers to the domain] to an Organizational Unit instead and moving the
>> groups and users into the OU that you want them to manage. --- Steve
>>
>> "From QC" <From QC@discussions.microsoft.com> wrote in message
>> news:1827439C-F403-44C3-AE7F-3BEEB8CD2C8B@microsoft.com...
>> > Hi!
>> >
>> > I need your help to determine what kind of permissions I need to give
>> > for
>> > a Network
>> > Technician on the domain:
>> >
>> > -Can log on the server
>> > -Can add computers in a domain
>> > -Can create a users and add to a specific groups
>> > -Can reset password
>> > -Cannot delete users
>> > -Cannot install applications
>> >
>> > This is what a need. I don't want to give user's total access(just the
>> > list higher) but enough to allow him to do his normal job.
>> >
>> > I know the custom permissions for a user, but anybody have a kind a
>> > recipe
>> > for what I need? If anybody use this kind of user in his network tell me
>> > what you do for this kind of user!
>> >
>> > Thanks
>> >
>> > Ans.:
>> >
>> >
>> > Look into AD delegation, though you may need to do some custom
```

microsoft.public.win2000.security: Re: Custom rights

>> > delegation.
>> You can
>> > modify the user right to logon locally to allow a user to logon to a
>> computer and you
>> > can give a user the right to create computer objects in the domain or
>> > OU
>> which would
>> > take care of the first two.
>> >
>> > Create a test OU and then select properties delegation to start the
>> delegation wizard
>> > to see what the "built in" rights are including resetting passwords and
>> modifying
>> > group membership and for the rest you will have to experiment with such
>> > as
>> the
>> > ability to create a user but not delete one would need to be a custom
>> delegation for
>> > creating user objects. The links below may help. --- Steve
>> >
>> >
>> <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/qp/526.asp>
>> >
>> > --- refer to the last paragraph
>> > <http://support.microsoft.com/default.aspx?scid=kb;en-us;294952>
>> > -- example of custom delegation.
>>
>>
>>