

# Re: how to restrict users to search in their own Organizational Unit

---

*Source:*

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active\\_directory/2006-12/msg00907](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2006-12/msg00907)

---

- *From:* "Jorge Silva" <jorgesilva\_pt@xxxxxxxxxxxx>
  - *Date:* Tue, 12 Dec 2006 23:49:04 -0000
- 

Ok

Let me start by saying that I only knew the real scenario after Lao's second post.

I also want to say that in fact you shouldn't deny the read permission to anyone and this scenario the MOSS Administrators or who is responsible for Add users to Your Sites should be careful when performing this action.

Now, because you're dealing with many users, my recommendation is to create THE NECESSARY Security Groups in each OU and related them with your MOSS2007 existing security groups, in future when someone creates some user, you just have to add that user to the necessary group and that user will be given the necessary permissions.

I would like to say that Herb's suggestion doesn't sound an easy or Fast solution, or more reliable than mine and sometimes can lead you to other problems, without going into deep on this I would like to say to Herb that maintaining the User group membership isn't not so hard, Lao can always create a UserModel in the correct OUs and Just copy it from there, if the user is in the correct groups it will be created with the necessary groups.

—  
\*\*\*\*\*

I hope that the information above helps you  
Good Luck

Jorge Silva

MCSA + Exchange + MSCE  
\*\*\*\*\*

"Herb Martin" <news@xxxxxxxxxxxx> wrote in message  
[news:eRkDTqhHHHA.1188@xxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:eRkDTqhHHHA.1188@xxxxxxxxxxxxxxxxxxxxxxxx)

Just set up delegated permissions to deny read acces for the users to the specific OU's

That was Jorge's original suggestion but it is not a simple matter (that is, no "just set up").

Who would you DENY? (Authenticated users or

Re: how to restrict users to search in their own Organizational Unit

Everyone would include Admins and the system itself.)

Jorge indicated creating a group, but doing that is non trivial -- how do you maintain this group -- and the poster has MANY OUs and thus needs many such groups to restrict access for each set to only the group created for each OU.

This is NOT an easy problem, but once the solution is decided a script can make it possible to accomplish, even if it is messy and ugly.

Again, I recommend against the idea, but there is certainly no "just" involved.

--

Herb Martin, MCSE, MVP  
Accelerated MCSE  
<http://www.LearnQuick.Com>  
[phone number on web site]

"MPerrault" <mperrault@xxxxxxxxxxxxxxxx> wrote in message  
<news:1165944097.876342.276440@xx>

Herb Martin wrote:

- > But, we have +/- 40 OU's with approximately 12000 users, how can I
- > handle this problem best?
- > If I need to create a security group per OU and then add all users
- > seperately then I will have alot of work...

Although I think the whole thing is a poor idea the most likely approach to make this practical is to write a SCRIPT.

[Admins need to be at least minimally competent at scripts writing so that at least they will know the basics and can get a true programmer to write the hard ones.]

You could also TRY removing the "Authenticated Users" (technically it isn't Everyone with these permissions) at the Domain level (and propagating) since using a lot of DENY permissions is in and of itself a poor practice.

Even then, I suspect something will/might go wrong so try this in a test domain, OR see if some AD expert will comment who has actually DONE such things. (Windows

Re: how to restrict users to search in their own Organizational Unit

has a bad habit of going south when such sweeping changes are made even though in principle they are perfectly logical.)

General script logic:

Loop through each (top level) OU

- 1) removing Auth. Users from permissions\*
- 2) create group of with OU users as members\*\*
- 3) add this group to permissions for this OU

\* Watch out for the effect on COMPUTER accounts etc. (Unless this is a test domain, I would likely REPLACE the Authenticated User permissions with an empty, 'place holder' group so that putting this stuff back would be practical.)

\*\* Must be maintained over time by 1) creating a template group and always created users through copying this with OU-group membership OR by scripting creation of users with this membership as there is no built-in mechanism for granting/denying permissions based on "OU" and these groups are a (semi-)manual thing.

You might have to periodically re-run this script to rebuild the groups to prevent discrepancies from growing over time (e.g., as users are moved from one group to another.)

--

Herb Martin, MCSE, MVP  
Accelerated MCSE  
<http://www.LearnQuick.Com>  
[phone number on web site]

<lao.nightwolf@xxxxxxxx> wrote in message  
<news:1165933306.200588.167530@xx>

>

> Jorge Silva schreef:

>

>> Hi

>> By default evryone has read-access to AD.

>> To deny that right you must create a security group and deny read

>> permission, then add the users to that security group.

>>

>> --

>>

\*\*\*\*\*

>> I hope that the information above helps you

>> Good Luck

Re: how to restrict users to search in their own Organizational Unit

```
>>  
>> Jorge Silva  
>>  
>> MCSA + Exchange + MSCE  
>>  
*****  
>>  
>  
> Thanks that helps already!  
>
```

Just set up delegated permissions to deny read access for the users to the specific OU's

Michael P. Perrault  
MCSE, CCNA, A+, MBA  
Senior Systems Engineer,  
ScriptLogic Corporation

Michael.Perra...@xxxxxxxxxxxxxxxxx  
www.scriptlogic.com  
<http://groups-beta.google.com/group/scriptlogic-desktop-authority>