

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/msg00859

- *From:* "Herb Martin" <news@xxxxxxxxxxxxxxxx>
 - *Date:* Tue, 12 Dec 2006 10:31:10 -0600
-

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 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

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

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

Jorge Silva

MCSA + Exchange + MSCE

Thanks that helps already!