

## Re: Create restricted user account, 2003 server AD domain

*Source:* <http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2005-11/0141.html>

---

*From:* Jim Fischer ([jfischer\\_link5809@now.here.com](mailto:jfischer_link5809@now.here.com))

*Date:* 11/14/05

Date: Mon, 14 Nov 2005 13:46:55 -0600

Thanks for the info, Steve and Roger. Your suggestions helped me find the next puzzle piece, I think.

I originally created the security group 'def' as a domain local group. With this configuration, here's what I see when user 'abc' logs on to an XP host in the domain and runs the 'whoami' utility (the AD domain name is 'demo'):

```
C:\Program Files\Support Tools>whoami  
demo\abc
```

```
C:\Program Files\Support Tools>whoami /groups
```

```
[Group 1] = "demo\Domain Users"  
[Group 2] = "Everyone"  
[Group 3] = "BUILTIN\Users"  
[Group 4] = "NT AUTHORITY\INTERACTIVE"  
[Group 5] = "NT AUTHORITY\Authenticated Users"  
[Group 6] = "LOCAL"
```

Note that user 'abc' is NOT listed as a member of the domain local group 'demo\def'. (And I did verify that the "Deny log on locally" right was applied to the domain local group "demo\def", and not to a machine local group(?) "def". I verified this on both the domain server and the XP hosts in the domain.)

If I recreate group 'def' as a global group and update everything accordingly (e.g., add user 'abc' to the global group 'def'; re-apply the "deny log on locally" right to the global group 'def'; run 'gpupdate /force' on the server & domain hosts), user 'abc' is now denied logon rights on the XP hosts within the domain.

So I guess now I need to find some useful definitions for domain local, global, and universal groups. Apparently, the information I read in various Microsoft Press books on Windows Server 2003, Windows XP, and on Microsoft's website wasn't clear enough to help me avoid this sort of configuration snag. FWIW, I found the following info regarding domain local groups at the

'informit.com' website:

<quote>

<http://www.informit.com/guides/content.asp?g=windowsserver&seqNum=45&r=1>

Domain local groups can be created and used only on domain controller computers. They're analogous to local groups on workstations: They're known only to computers holding the account database (domain controllers), and can therefore be applied only to resources on those computers.

</quote>

The key phrase here seems to be "on those computers" in the last sentence. The 'whoami' output shown above seems to corroborate this, in that the XP hosts in the domain apparently have no idea that user 'abc' is a member of the domain local group 'def' (i.e., demo\def). In other words, the domain controller knows that 'abc' is a member of the domain local group 'def', but the domain hosts do not. In your opinion, is the description from the informit.com website a more-or-less accurate description of what domain local groups are used for – i.e., applying policy to resources located ONLY ON the domain controller computers themselves (e.g., a printer server service running on a domain controller), and not to resources residing in the domain in general?

Jim

"Steven L Umbach" <n9rou@nospam-comcast.net> wrote in message news:OR3Vy175FHA.1148@tk2msftngp13.phx.gbl...

> *It should work with a security group and I suggest you use global groups as the security group for what you want to do. It could be for some reason the user's security token has not been updated yet when he logged onto the XP Pro computer [cached credentials maybe] or the security policy change had not yet propagated. I would check Local Security Policy on the XP Pro computer to make sure your group shows in the user right for deny logon locally. If the user still can logon use the support tool whoami /groups to see if his security token shows the group that is listed in the deny logon user right. Also FYI in Windows XP Pro you can use rsop.msc to see the current Group Policy settings applied to the computer and logged on user and from what GPOs the settings came from. --- Steve*

>

>

> *"Jim Fischer" <jfischer\_link5809@now.here.com> wrote in message news:%238ApPL15FHA.1184@TK2MSFTNGP12.phx.gbl...*

>> *Doh! I just figured out one of the missing puzzle pieces. Changes made to the security policy are not necessarily applied immediately. (Note to self: Some factors that affect the current GP settings: GP updates are pushed only periodically, ~90 minutes; logout/logon; reboot.)*

>>

>> *After I applied the domain security policy "Deny log on locally" to user 'abc', I ran the program 'gpupdate.exe' on the active directory server AND on all of the XP hosts in the domain to manually update the group policy settings on those machies. That did the trick. User 'abc' can no*

>> *longer log on to the XP hosts in the domain.*  
>>  
>> *What I'm trying to figure out now is how to apply the domain security*  
>> *policy "Deny log on locally" to the members of a security group. Here's*  
>> *what I tried:*  
>>  
>> *\* I removed the domain security policy "Deny log on locally" from the*  
>> *user 'abc'.*  
>>  
>> *\* I ran 'gpupdate' on the domain controller and the XP hosts in the*  
>> *domain and verified that I could once again log on to the XP hosts as*  
>> *user 'abc'.*  
>>  
>> *\* On the domain controller I created a security group 'def' and added the*  
>> *user 'abc' to that group.*  
>>  
>> *\* On the domain controller I applied the domain security policy "Deny log*  
>> *on locally" to group 'def'.*  
>>  
>> *\* I ran 'gpupdate' on the domain controller and the XP hosts in the*  
>> *domain.*  
>>  
>> *When I tried logging on to an XP host as user 'abc', I was successful.*  
>> *<sigh> So what am I missing here??? Why can user 'abc' still log on to*  
>> *the XP hosts in the domain when user 'abc' is a member of the security*  
>> *group 'def', and security group 'def' has the domain security policy*  
>> *"Deny log on locally" applied to it???*  
>>  
>>  
>> *Jim*