

Re: Restricted Groups – Local Users Group

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.group_policy/2005-10/msg00197.html

- *From:* "Steven L Umbach" <n9rou@xxxxxxxxxxxxxxxxxxxx>
 - *Date:* Fri, 14 Oct 2005 21:10:04 -0500
-

Glad you got it sorted out though that alone would not explain why a regular user seemed to have administrator powers. It probably is of little use to try and use Restricted Groups to restrict the user local group on a domain computer and best left to manage privileged groups. Keep in mind that you can also configure the user rights for logon locally and access this computer from the network to control what users/groups have interactive or network access to the domain computers. --- Steve

"jmalloney" <jmalloney@xxxxxxxxxx> wrote in message

news:eF49Y0LOFHA.1028@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

> OK well I figured it out. When I added domain users to the local users
> group via Restricted Groups the policy removed the default INTERACTIVE and
> AUTHENTICATED USERS from the local users group. After I added the groups
> back into restricted groups my policy worked fine.

>

> Thanks for all your help!!

>

> "Steven L Umbach" <n9rou@xxxxxxxxxxxxxxxxxxxx> wrote in message

> news:um%23T6AE0FHA.664@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

>> Interesting. Verify that the regular user that you believe has excessive
>> access can run the command secedit.msc to open and edit Local Security
>> Policy. Double check with the command "net localgroup administrators"
>> that only the administrator and domainname\domain admins group is listed
>> as members. Then logon to the computer as the local administrator [non
>> domain account] to verify that the local administrators group has the
>> SID of BUILTIN\Administrators" S-1-5-32-544 by using the command whoami
>> /groups /sid. Whoami is part of the support tools. Logon as the domain
>> user who you believe to have excessive access and run the command whoami
>> /user /groups to check the group membership of his access token to see if
>> it is what you expect. Then run the command net group "domain admins" on
>> a domain controller to see if it is what you expect and remember any
>> domain user that is also in the domain admins group either directly or
>> via group nesting will be a local administrator on the domain computers.
>> On the domain workstation computer check the security logs for anything
>> unusual around the time you were logged on as a regular domain user after
>> making sure that auditing of logon events and account management is
>> enabled. If still nothing seems to explain your problem, move a domain

Re: Restricted Groups – Local Users Group

>> computer into an OU that is not using Restricted Groups and remove
>> everyone but the built in local administrator account from the local
>> administrators group and then logon to that computer as a regular domain
>> user to see what happens. --- Steve
>>
>>
>> "jmalloney" <jmalloney@xxxxxxxxxx> wrote in message
>> news:%23HOv6iC0FHA.1256@xxxxxxxxxxxxxxxxxxxxxxxxxxxx
>>>I ran all commands and the result is the same as what I see in Users and
>>>Groups. Everything appears to be configured correctly. Again all
>>>"domain users" are in the local users group only, yet anyone who logs in
>>>appears to have local admin rights to the pc!!
>>>
>>> "Steven L Umbach" <n9rou@xxxxxxxxxxxxxxxxxxxx> wrote in message
>>> news:ertFZGC0FHA.1256@xxxxxxxxxxxxxxxxxxxxxxxxxxxx
>>>> Something seems to be amiss. On a computer where this is happen use the
>>>> command net local group administrators to see exactly what users and
>>>> groups are in the local administrators group and for a user in question
>>>> run the command net user username to see the group memberships of the
>>>> user named in username. If you have any questions about the results of
>>>> those commands post the results here in a reply. Also in Active
>>>> Directory Users and Groups check the membership of the domain admins
>>>> group to make sure it is what you expect. --- Steve
>>>>
>>>>
>>>>
>>>> "jmalloney" <jmalloney@xxxxxxxxxx> wrote in message
>>>> news:%23uhYMJA0FHA.1924@xxxxxxxxxxxxxxxxxxxxxxxxxxxx
>>>>>I have used restricted groups in GP to control membership of both the
>>>>>local users and administrators groups. I added the "domain users"
>>>>>group to "Users" and "Domain Admins" group to "Administrators". The
>>>>>main reason I did this was that I wanted all domain users to be
>>>>>restricted from making system-wide changes to their local pc. The
>>>>>policy worked as I could see that their local groups reflected my
>>>>>settings at the domain. The problem is that although domain users are
>>>>>in the "users" group they are still able to make system-wide changes.
>>>>>I tested this, as a user I can make myself a local admin, delete system
>>>>>files...etc...
>>>>>
>>>>> In the past I never used group policy for this. I would simply open
>>>>> control panel, users, and add the user to the "restricted users"
>>>>> group. This always worked well, and prevented them from making any
>>>>> critical changes to the system. My understanding was that the "users"
>>>>> in computer management was the same as the "restricted users" group
>>>>> shown in control panel\users. What am I doing wrong?? I want all my
>>>>> domain users to be restricted through group policy!!
>>>>>
>>>>> HELP!
>>>>>
>>>>>
>>>>>

Re: Restricted Groups – Local Users Group

>>>
>>>
>>
>>
>
>

• **References:**

- ◆ **Restricted Groups – Local Users Group**
 ◇ From: jmalloney
 - ◆ **Re: Restricted Groups – Local Users Group**
 ◇ From: Steven L Umbach
 - ◆ **Re: Restricted Groups – Local Users Group**
 ◇ From: Steven L Umbach
 - ◆ **Re: Restricted Groups – Local Users Group**
 ◇ From: jmalloney
- Prev by Date: **Re: Hang @ Applying Computer Settings/Applying Your Personal Setti**
 - Next by Date: **Re: Software Distribution using Group Policy**
 - Previous by thread: **Re: Restricted Groups – Local Users Group**
 - Next by thread: **Re: Local GP for just 1 user**
 - Index(es):
 - ◆ **Date**
 - ◆ **Thread**