

# Re: Disabling Interactive Logon Against Security Group

---

*Source:* <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2006-08/msg00464.html>

---

- *From:* "Roger Abell [MVP]" <[mvpNoSpam@xxxxxxx](mailto:mvpNoSpam@xxxxxxx)>
  - *Date:* Mon, 14 Aug 2006 21:24:29 -0700
- 

A less than fully perfect route to consider would be a logon script for those accounts that inquires as to what machine is being logged into and bails/logsoff if it is not one in the short list.

That could get you by for the time being while you use sequence of machine startup script, or remote admin script, to alter user rights by use of ntrights.exe (from resource kit, on share accessible to Domain Computers group).

Roger

"Sam Gaw" <[SamGaw@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:SamGaw@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)> wrote in message [news:05F10108-F297-4A34-A47B-564859EA0151@xxxxxxxxxxxxxxxxxxxx](mailto:news:05F10108-F297-4A34-A47B-564859EA0151@xxxxxxxxxxxxxxxxxxxx)

Rgar,

Point taken; I'm being to accept that this is going to be my only solution to the problem even though I'd of preferred a method of approaching this from a user account basis rather than machine basis.

Appreciate your time & help, and everyone else's on this.

--

Regards,  
Sam Gaw

<http://www.samgaw.co.uk>

"Roger Abell [MVP]" wrote:

"Sam Gaw" <[SamGaw@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:SamGaw@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)> wrote in message [news:DEC97BE9-A4C5-464E-9755-536F208A43BF@xxxxxxxxxxxxxxxxxxxx](mailto:news:DEC97BE9-A4C5-464E-9755-536F208A43BF@xxxxxxxxxxxxxxxxxxxx)

Re: Disabling Interactive Logon Against Security Group

Thanks for the replies, to be honest though I was hoping to avoid this approach which is why I wasn't quite sure of the initial reply.

Essentially this is to secure half a dozen guest accounts on domain of 50,000+ so that they may access a web app so to modify the security policies this way is in my opinion a little drastic and why I original phrased my question "disable interactive logon privileges against specific OU/User Groups rather than against computers?"

I haven't had a chance yet but when I return to the office tomorrow I was thinking of creating the accounts in the same sort of manner as I would a service account given that other than SQL it's possible to prevent interactive logons with DSAs.

Has anyone tried this before? I had assumed that this would have been fairly common practice in anywhere that followed least-privileged designs.

Hi Sam,

I hope you catch some other replies, with good methods. Where I follow least privilege this is a total non-issue, as the machines are not left at default with Domain Users and Authenticated Users in Users and with logon rights granted to Users. IOW, in that deployment if the account is not added to a group that does grant login to a set of machines they cannot. For your current issue, problem solved.

Roger

"Roger Abell [MVP]" wrote:

Re: Disabling Interactive Logon Against Security Group

Paul has shown you where to locate that policy.

There are however some potential issues to consider.

If you set this in a GPO then the list that is to be denied that you provide in that GPO is the one, complete list used for that user right setting on all machines subject to that GPO. In other words, if this setting is being used on some machines, the value provided in the GPO will replace what exists on those machines. If you look, this is used in a default on XP clients for a couple/few accounts, so those would no longer be denied after the GPO is applied if your GPO just says to deny your CustomWebUser group.

One route to avoid this is to cause a machine local group to be defined on each machine "DenyLocalLogin" and placed into the machine's user right to deny interactive login. Then, you can control the membership in this machine local group using the restricted group capability from your GPO. Similar to the issue with the user right, if you do not want to have your GPO take control over the complete and total membership in the machine local group then you can use technique outlined in this KB <http://support.microsoft.com/kb/810076>

"Sam Gaw"

<SamGaw@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>  
wrote in message

[news:52FDD057-DCD7-4A21-AD50-3F3DA71CB191@xxxxxxxxxxxxxxxxxxxx](mailto:news:52FDD057-DCD7-4A21-AD50-3F3DA71CB191@xxxxxxxxxxxxxxxxxxxx)

Svyatoslav,

Re: Disabling Interactive Logon Against Security Group

Thanks for getting back to me so quickly; I'd thought about that myself but the problem is I can't actually find the policy anywhere. Any ideas?

--  
Regards,  
Sam Gaw

<http://www.samgaw.co.uk>

"S. Pidgorny <MVP>"  
wrote:

Add the group containing to the "Deny log on locally" policy on the domain level?

--  
Svyatoslav  
Pidgorny,  
MS MVP –  
Security,  
MCSE  
–= F1 is the  
key =–

"Sam Gaw"  
<SamGaw@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>  
wrote in  
message  
<news:AFEC2F64-F0D4-42B1-A8AF-E461165911D4@xxxxxxxxxx>

I  
was  
wondering  
if

Re: Disabling Interactive Logon Against Security Group

anybody  
knew  
of  
a  
way  
to  
disable  
interactive  
logon  
privileges  
against  
specific  
OU/User  
Groups  
rather  
than  
against  
computers?

Essentially  
I  
want  
to  
be  
able  
to  
provide  
domain  
accounts  
to  
users  
to  
access  
a  
web  
app  
published  
on  
the  
WAN  
but  
prevent  
them  
from  
accessing  
the  
domain  
via  
any  
of  
our

Re: Disabling Interactive Logon Against Security Group

computers/interactive  
logon.

Any  
help  
or  
advice  
would  
be  
much  
appreciated.

--

Regards,  
Sam  
Gaw

<http://www.samgaw.co.uk>