

## Re: How can admin not have access to certain shares?

---

*Source:*

<http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2008-02/msg00083.html>

---

- *From:* "Anthony [MVP]" <[anthony@xxxxxxxxxxxx](mailto:anthony@xxxxxxxxxxxx)>
  - *Date:* Mon, 25 Feb 2008 14:41:35 -0000
- 

We are probably talking about different scale, and I suppose the only useful question is whether the OP has an answer.

I notice that your solution requires a separate domain and different domain admins. Not sure how that differs from the problem you identified with the separate workstation (or domain if on a larger scale).

Anthony

<http://www.airdesk.com>

"DaveMo" <[david.mowers@xxxxxxxx](mailto:david.mowers@xxxxxxxx)> wrote in message

<news:735dd5d7-c112-4a69-9655-009efd4964e2@xx>

On Feb 25, 2:29 am, "Anthony [MVP]" <[anth...@xxxxxxxx](mailto:anth...@xxxxxxxx)> wrote:

I think that's a bit over the top.

In the real world, I am guessing that perhaps a business owner or director is hiring a system administrator but wants to have some data that is private. It could be the Finance Director. The question is, can this be done

within a domain? The answer that I and others have given is:

- You can remove access, but the admin can take it back
- You can audit access, but the admin can change the auditing.

So if you really don't want the admin to have access to the data you need to

store it outside of the domain he is administering. For example, on a workstation. Then back up the workstation.

Anthony <http://www.airdesk.co.uk>

"Al Dunbar" <[AlanD...@xxxxxxxx](mailto:AlanD...@xxxxxxxx)> wrote in message

<news:%231HuGXdIHA.4260@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>

"Anthony [MVP]" <[anth...@xxxxxxxx](mailto:anth...@xxxxxxxx)> wrote in message  
<news:%231CbOwMdiHA.2404@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>

Re: How can admin not have access to certain shares?

If you want data to be outside the scope of a domain administrator, it is fairly obvious that you need to put the data outside the domain.

Brilliant! But then what is the security environment of this data repository that is outside the domain? Is it another domain with a different set of administrators? Is it a SAN device on the network? Is it a vault containing the data on magnetic media or printed reports?

And if the data is ever processed by any machine actually \*on\* the network, what process ensures that it is inaccessible to anyone other than the authorized user while in use, and fully deleted once he files the results away in that magical non-domain world?

You can certainly use such techniques to keep system admins from having any sort of access to the information. But I am not convinced that the data itself will become any more secure from unauthorized access in general as a result.

Auditing the data so that you are alerted when someone accesses it is different. It is like putting the burglar in charge of setting the alarm.

If that is truly the case, then we must immediately stop all auditing of security events, as this has no place in securing our data. Much better to hide the data in a sock in the mattress in your spare bedroom where you cannot possibly audit the situation, and can therefore be sure that no knowledge will ever come your way of its having been accessed. In a nutshell, you will have then proven it is perfectly safe.

/Al

Re: How can admin not have access to certain shares?

Anthony  
<http://www.airdesk.com>

"Leythos" <v...@xxxxxxxxxxx> wrote in message  
<news:MPG.222775611d99c0d2989a6e@xxxxxxxxxxxxxxxxxxxxxxxx>  
In article <1a3d0a6f-760d-4fbd-b134-cad4303349c3  
@z17g2000hsg.googlegroups.com>,  
david.mow...@xxxxxxxxxxx says...

On Feb 21, 7:36 am, Leythos  
<v...@xxxxxxxxxxx> wrote:

In article  
<7a2dcc1d-2c71-4e9a-a6c3-1b2514b2fdb6@  
71g2000hse.googlegroups.com>,  
david.mow...@xxxxxxxxxxx  
says...

Through a  
combination  
of setting  
the  
correct  
policy (no  
access for  
admins) and  
then  
monitoring  
the  
systems  
so that the  
policy does  
not change,  
you can  
achieve the  
desired  
compliance  
level for  
your  
systems.

Actually, that does not meet  
the requirement – the  
requirement was  
to

Re: How can admin not have access to certain shares?

block access by Admins to a  
share/file/folder/etc...

It can not be done.

Yes, you can provide a log  
that the violation has  
happened, but you  
can  
not stop it.

I don't think that you are accurately  
representing the problem and/or  
possible solutions. Given that there are  
fundamental issues with  
keeping an admin from doing anything on  
his box, this does not mean  
that there aren't things you can do to make a  
system more secure or  
more compliant. Doing something is almost  
always better from both a  
security and compliance perspective than  
doing nothing at all.  
Compliance inspections are never binary in  
either their goals or their  
results. Since no system is ever completely  
protected no company would  
ever pass a security audit if the requirement  
was to provide bullet  
proof security.

In summary, adding systems that provide  
monitoring and policy  
enforcement will definitely tend to make an  
organization more likely  
to be found "in compliance" than doing  
nothing at all.

This is, of course, the view of a system  
implementor. If there are  
compliance folks out there who would like

Re: How can admin not have access to certain shares?

to comment, their  
contributions would be welcome.

Dave, I work for many clients, and many of them have to  
provide SOX or  
other compliance proof.

The simple fact is that no matter how you dice it up, if you  
have  
domain  
admin access you have access to everything and there is no  
way to  
change  
that.

Yes, logging can show that an admin violated security, but  
that doesn't  
change the specifics – the admin has access to anything they  
want  
access  
to, period.

Your Usenet client is broken, it's not properly clipping  
signature  
lines  
when you reply.

--

Leythos  
– Igitur qui desiderat pacem, praeparet bellum.  
– Calling an illegal alien an "undocumented worker" is like  
calling a  
drug dealer an "unlicensed pharmacist"  
spam999f...@xxxxxxxxxxx (remove 999 for proper email  
address)– Hide  
quoted text –

Re: How can admin not have access to certain shares?

– Show quoted text –

I'm sorry, but I can't agree that this approach is a good one. Who is going to administer the separate workstation? The Finance Director? If the workstation is not a member of a domain, it will not enjoy the benefits of whatever domain-based policies that are used to keep the organizational systems healthy. If it is outside of the domain, the Finance Directory won't be able to access the data using his domain account so he'll need to manage another account – and probably keeping the account info on a sticky note on his monitor!

There are audit collection systems widely available that whisk the audit log events off of a box in real-time. Critical audit information, such as access info for your highly confidential data in this scenario is then collected in a database on another system which can be under the control of a different group of admins responsible for enforcing compliance. Like anything else, any mechanism could be subverted if someone is really, really smart and motivated to do so, but I think that a combination of such technologies will easily prove due diligence and get you past the audit.

Dave

.