

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

---

*Source:*

<http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2008-02/msg00072.html>

---

- *From:* Leythos <void@xxxxxxxxxxx>
  - *Date:* Thu, 21 Feb 2008 11:48:27 -0500
- 

In article <1a3d0a6f-760d-4fbd-b134-cad4303349c3@z17g2000hsg.googlegroups.com>, david.mowers@xxxxxxxx says...

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

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

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

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 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"

spam999free@xxxxxxxxxx (remove 999 for proper email address)

.