

Re: how can I stop user deleting important files

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2005-09/msg03865.html>

- *From:* Wood Contour <none@xxxxxxx>
 - *Date:* Wed, 21 Sep 2005 06:15:04 GMT
-

Bharat wrote:

Thanks I'll give it a go.

Just tried this at home on an XP Pro PC (no Windows Server in the mix)
Setup a new User "Test" with USER privileges only..

Guess what - I can delete BOOT.INI and NTLDR etc whilst logged in as TEST
boy I need to investigate this a bit more

"MCSEGURU" <mcseguruhere@xxxxxxx> wrote in message
[news:OmRxs\\$cvFHA.4032@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:OmRxs$cvFHA.4032@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)

Unless your default NTFS Permissions on your PC are jacked, Domain Users
shouldn't have access to modify or local system files on their PC. Are

you

sure they aren't members of their PC's
Administrators group. Even though

you

have given them de-elivated permissions from the
SBS Domain Directory,

that

doesn't necessarily override their permissions on their local PC's.

If it may be that they are elevated on the local PC's as a result of
Administrator group memberships, try enforcing restricted "Administrators"

Re: how can I stop user deleting important files

to the Local PC's using Group Policies.

In Server Manager, Advanced Management, Group Policy Management, Your Forest, Your Domain, Your Domain.local, Default Domain Policy (right click and select Edit), Computer Settings, Windows Settings, Security Settings, Restricted Groups, Add Group, Administrators, Add Users... etc...

Make sense? This will propagate specific users to be members of the Administrators Group on your domain member computers.

"Bharat" <bharat@xxxxxxxxxxxx> wrote in message
news:utTDrtcvFHA.252@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Setting up user as USER - still allows them to delete

NTLDR
BOOT.INI
etc.....

So something is wrong. You can resort though to the group policy, assuming you have dealt with policies before. May I suggest that you create a test directory on at least one target machine. Create a directory called test on a test machine, and create one on yours. Open Computer configuration > Windows Settings > Security settings > file System. Add a directory or a file that you would like to protect and assign the permissions when prompted. Make sure that the user belongs to the organizational group your assigning the policy to, and if you will, you create a test one too. Once you put the policy in place, either log the user on and off, or simply execute GPUPDATE on his machine and test it. I use this area company wide to allow specific users deleting accounting log files and allow only managers to delete by looping policies.

Re: how can I stop user deleting important files

Let us know how goes it.

--

Dana

<http://www.woodcontour.com>

Solid wood and stone PC Peripherals

.