

Re: preventing access to the c: drive...

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.terminal_services/2009-03/msg00049.html

- *From:* "TP" <tperson.knowspamn@xxxxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 4 Mar 2009 08:49:18 -0500
-

Hi Vera,

I wonder if Brad has actually checked whether or not users have the ability to create folders **anywhere**?

I think maybe he is confused because the default permissions allow users to create files/folders on the root of C: as well as browse most folders (except other user profiles).

Changing the default permissions to the root is something I do on every TS. I change it so that normal users have Read & Execute applied to This folder only for the root.

Note to Brad: make sure you understand NTFS permissions before doing this—I am **not** replacing permission entries on child objects, only the root.

One common configuration for the root will look like this:

Allow Administrators Full Control This folder, subfolders and files
Allow SYSTEM Full Control This folder, subfolders and files
Allow Users Read & Execute This folder only

The net effect (besides preventing users from creating something in the root) of this is to change the root to more of a "secure by default" model. For example, if I create a new folder in the root normal users will not have access to it, because by default it will be assigned permissions of Administrators and SYSTEM Full Control.

On a TS with tighter security requirements I will use a similar technique, but applied to Program Files. I then have to manually grant groups permissions to the various subfolders. Time-consuming of course.

-TP

Vera Noest [MVP] wrote:

If users can create folders anywhere on your C: drive, then you are **not** using the default permissions. Part of those are:

%SystemDrive%, %SystemRoot%, %ProgramFiles%
and %SystemRoot%\system32 :
System – Full Control
Administrators – Full Control
Authenticated Users – Read & Execute

Re: preventing access to the c: drive...

Maybe you have also modified registry permissions?
In that case, you have partly bypassed Full Security, and that's not good.

Maybe you should load the default security template and compare your settings with the out-of-the-box settings and see what else is different.

Vera Noest
MCSE, CCEA, Microsoft MVP – Terminal Server
TS troubleshooting: <http://ts.veranoest.net>
___ please respond in newsgroup, NOT by private email ___