

Re: Deny _WRITE_ access to a file

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2005-03/0033.html>

From: Javier J (*no.mail_at_please.no*)

Date: 03/01/05

Date: Tue, 01 Mar 2005 20:50:29 +0100

Hi!!

Thanks a lot for the response.

First of all, regarding LOGON SCRIPT, the mistake is mine: What I was trying to talk about was a STARTUP script (if I'm not mistaken, that script runs as BUILTIN\SYSTEM).

I think I'd rather explain a bit more about the environment so that it's clear of why I'm asking for such strange things:

The situation is as follows: The PCs in question (Win 2000 PRO, SP4+, W2000 Mixed Domain) "belong" to a group of users who, as part of their normal duties, have to handle sensitive information using an internal company app. To avoid undue information leakage, these users have *TWO* logon users for the domain, a highly restricted one that is used to run the corporate app/access sensitive information, and a "Normal" user for the rest of everyday tasks.

The "normal" user can run all software EXCEPT the restricted app, and can work normally.

The setup for the restricted user (using GPO, crypto software et al) is such that the restricted user only can run the "sensitive" app, they can't browse or "see" in Explorer the local folders, their profile is redirected to an encrypted network etc etc...

Also, using an STARTUP batch script, the members of the restricted group have been DENIED access to different .exes that restricted users should not run (ftp.exe, telnet.exe and other) and folders they don't need access to. (Windows already protects system folders against accidental change). The problem is, there are a couple of folders on C:\ (such as c:\local_settings) that the user logon needs to be able to read, because it sets machine-specific config. (such as the building's mail server, the NT server, and suchlike)

The problem is that the folder is set to be writeable by "Everyone". I'd like to be able to "change" it so "no write" for the users of this

microsoft.public.windows.server.security: Re: Deny _WRITE_ access to a file

particular group. I can DENY access, but these users are part of "Everyone", so even if "RestrictedG" has only READ access, as they are members of "Everyone"; they get to write there...

Why am I exploring the "deny" route, instead of limiting the rights of "Everyone".. because there are some cases where the normal user has to be able to write, so "Everyone:W" is a valid permission.... as long as I could do something like "RestrictedG":DENY WRITE....

I know that permission is "settable" (is that a word?) as it can be set using (the "simple") NTFS Perms. tab... but to script it is what is driving me crazy!!

Thanks a lot. Any help _WILL_ Be more than welcome!!

Javier J

On Mon, 28 Feb 2005 22:12:30 -0700, "Roger Abell" <mvpNOSpam@asu.edu> wrote:

>Al is quite right in picking up on your mention of use in a
>login script – which skipped my attention.
>To do as you had planned you would need to do this in
>a startup/shutdown script, not login/logoff script.
>
>However, you really, really would IMO be better off by
>restructuring so that all files with this requirement are in
>a folder with appropriate grants, not mixed in with other
>files in a folder where the default NTFS permissions will
>need to be changed.