

Re: Passwords on Folders

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2004-02/0462.html>

From: *Vanguard* (no-email_at_no-spam.invalid)

Date: 02/09/04

Date: Mon, 9 Feb 2004 13:40:08 -0600

"Sal" said in news:ca8a01c3ef3c\$1f8238d0\$a101280a@phx.gbl:

- > *Does anyone know what are the pro's and con's of using*
- > *passwords on folders? Also, does NT/windows 2000 allow*
- > *you to use passwords on folders?*
- >
- > *I'm pretty sure using restrictions (Read, Write, Admin,*
- > *etc...) is the proper way to procedure but I would like*
- > *some insight on using passwords on folders if possible.*
- >
- > *Thank you.*
- > *Sal*

Windows NT/2000/XP do not natively let you set passwords on folders. There are products you can buy and install that will do that. For example, ZipMagic loads as an installable file system and makes .zip files look like folders (and you can password protect .zip files). That's just one way.

Setting permissions on folders and files is okay within the instance of Windows under which those permissions were defined. If you yank the drive out of the computer and plug it into another computer running Windows, most of the permissions are ignored. I think the Administrator account uses the same SID (security identifier) across all NT-based versions of Windows. However, any permissions based on user accounts won't be obeyed. The SID used to track permissions on a file as to which user has those permissions won't be known on the computer to where you hauled the drive. Since this other instance of Windows doesn't know about the SID, it cannot obey the permissions based on that unknown SID. You can also take ownership of the file so you can then delete the unknown SID and add your own permissions under that instance of Windows. So permissions are good but only while the drive is still under the instance of Windows where the SIDs were defined upon which those permissions were based. I suppose you could copy the SAM (Security Accounts Manager) file to the other computer but you would be sacrificing the SAM that was already there on that new computer (I haven't heard of a mans of merging SAM files).

For best protection, use NTFS on your hard drives so you can then EFS (Encryption File System). You can even configure EFS to allow only your

account to be able to read the folder and files and not let the Administrator read them. Administrator could still take ownership or modify permissions but it couldn't read the contents of the files. Be sure to export your EFS security certificate. If you move that drive with EFS-protected files to another computer (i.e., under a different instance of Windows that doesn't have your EFS certificate), or if you restore EFS-protected files from a backup onto a different computer, then you need to import your EFS certificate so you can read those EFS-protected files over there. If you don't export the EFS certificate, you have basically locked the files and thrown away the key, so hopefully that instance of Windows never has to be reinstalled or you don't have to move or restore the EFS-protected files to another and different instance of Windows.

EFS is the way to go if you want to prevent anyone but yourself to read the contents of your files even if you move the files to a different Windows host or have to reinstall Windows and restore your files. Never EFS protect the system files (i.e., don't apply EFS to %windir% or any subdirectory). There's no point to EFS protect executable files (i.e., .exe) unless the program is your own creation and you don't want anyone else to execute it or disassemble it. EFS incurs a slight penalty in time due to the delay to decrypt the file's contents.

--

*** Post replies to newsgroup. E-mail is not accepted. ***
