

# Securing a standalone workstation

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2004-09/1095.html>

---

**From:** Michael Quinlivan (*mq\_spam\_acct\_at\_hotmail.com*)

**Date:** 09/18/04

Date: 17 Sep 2004 20:29:04 -0700

Hi All

I am wanting to know if it is possible to acheive the following. I have a home computer that I want to share with others. Each user has there own local user account. The machine is connected to the Internet but is not on a domain. I want to be able to restrict them so that the only folder visible on the machine is their respective My Documents folder. I do this because firstly I want them to save all data in ONE area only, not all over the hard disk. Secondly, I don't want them to run certain programs. This means that they can only "see" files that they have created, and cannot browse to any other part of the filesystem. They are restricted to executing only those applications present on the Start menu.

I have attempted to do this, but ran into some obstacles. I tried using NTFS permissions to hide any folder and files except My Documents, but to fully acheive this hiding breaks the applications on the Start Menu. By disallowing them to see any files means that they can not run the applications because they are invisible!!

I then tried relaxing the permissions on those files and folders that are used by an application. This fixed the problem, but it now allows anybody to delete certain application files, especially with legacy applications. And what if I missed some files and programs that are legit? It just seems to be a lot of messing around to me. Does Windows have any concept of setuid, where you can run a program at a privileged level? That way I could just hide everything on the drive, exposing only application entry points that are run at a higher privilege level allowing the application to run properly. Only problem here is that if the application is running at higher privelege level, a Save As dialog box may allow you to save to some part of the file system that I don't want them to. Or are there any alternatives to Windows Explorer that let you restrict drive access?

It seems with Windows it is impossible to have absolute control over what happens, ther is always a compromise. Is this the case, or am I just not knowledgeable enough about it? It seems all this would be solved by simply having a server/shared drive where al documents can

microsoft.public.security: Securing a standalone workstation

be kept, and then just restricting access to C drive via Local Machine Policy...

thanks in advance...