

## Re: Default Shares

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2005-10/0314.html>

---

**From:** Steven L Umbach (*n9rou\_at\_nospam-comcast.net*)

**Date:** 10/24/05

Date: Mon, 24 Oct 2005 13:16:38 -0500

I would not worry too much about disabling the default shares if they are going to make your jobs more difficult and they should not be disabled on domain controllers. Instead focus on using very strong passwords and training domain level administrators to never use their domain level administrator account to logon to any domain computer that is not known to be 100 percent secure as in free from keyboard loggers, malware, malicious scripts, etc. Instead create regular domain user accounts that are in the local administrators group of domain computers which can be easily managed via Group Policy Restricted Groups and tell them to make sure they do NOT use the same password as they use for their domain level administrator account. Sensitive servers should have a different global group of domain user accounts in their local administrators group for management than the regular domain workstation population to further isolate them in case of the capture of credentials via a domain workstation or a worm infection that may try to access administrative shares. Regularly reviewing of your security logs can also detect failed logon attempts [assuming auditing is enabled] and questionable logons such as an administrator accessing a computer from a workstation that they should not be or at strange days/times.

This is something to consider. Even if the administrative shares are disabled a user could still use something like psexec to access the command prompt of a server remotely if they knew administrative credentials. You should also consider implementing ipsec to protect domain computers including from each other if there is no reason for particular domain computers to access other domain computers for any reason. Ipsec is somewhat complex and requires a lot of planning, testing, and exempting domain controllers from ipsec policies that would otherwise cause them to try to use ipsec between themselves and domain computers which can cause huge problems in the domain. Microsoft has an excellent white paper on using ipsec for domain isolation at the link below. Windows 2003 and XP Pro computers can also take advantage of the Windows Firewall to manage what traffic a computer can accept and from what IP addresses being managed by Group Policy. Ipsec "filtering" policies can also do much of the same for Windows 2000. --- Steve

<http://www.sysinternals.com/Utilities/PsExec.html> --- psexec.

<http://www.microsoft.com/technet/security/topics/architectureanddesign/ipsec/default.mspx>  
--- Server and Domain Isolation Using IPsec and Group Policy

"nospam" <bluetooth995@gmail.com> wrote in message  
news:1130160678.673165.62990@g47g2000cwa.googlegroups.com...

> *Hi all,*

>

> *Any secure practices would recommend you to*

> *disable all the windows default shares –C\$.Admin\$*

>

> *Of course, this is going to create problem for the system*

> *administrator – this limit their ability to*

> *manage the system with WMI, remote access,etc...*

>

> *So, if the admininstrator is having a strong password*

> *does it somehow mitigate the risk of having default shares?*

>

> *I would normally think defense in depth – though admin with*

> *strong password, but shnd still disable default shares*

>

> *Any comments?*

>