

RE: Any way to remove ADMIN\$ only?

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2002-11/0031.html>

From: jmcguire@sbc.com

Date: 11/07/02

To: Evan Mann <emann@questinc.org>
From: jmcguire@sbc.com
Date: Thu, 7 Nov 2002 10:22:54 -0500

Been a while since I locked up a Terminal server which is the only time I really go to this level of local security given my current customer base, but let me try to remember. First of all, you must have NTFS on the system partition to allow you to set local permissions. Users can normally function with read only to the system drive with the exception of their profile and temp folders. For temp folders, give the users local group change. Give each individual user Change access to their own profile (documents and settings in 2k+) or better yet, if the situation allows, use roaming profiles or mandatory profiles and handle the permissions on the server. Make sure you give administrators full control to all (including program files) in your settings though, or the next service pack upgrade won't go well (voice of experience :-)

This will keep them from installing apps and deleting files. Your "know enough to be dangerous" users that actually have some skills may find some way past this cursory protection. System policies and additional registry permissions may be required to handle your particular user base. This also depends on a rather simplistic view and gets much more complicated if you have help desk types that need install privileges, but may still screw something up if given too much access. Also, custom apps and many poorly written line of business apps (read most) may store working files in the application directory and require an install on the C: drive. This is fortunately easy to test in most cases as the apps at least throw an error and at best will show you what file it tried to write in.

As always, YMMV so anyone else is free to add to this or correct me.

JOHN MCGUIRE CISSP, MCSE2k, MCSE+I, MCT
Network Security Specialist
888.529.0401
jmcguire@sbc.com
Strictly Business
www.sbc.com

Evan Mann

RE: Any way to remove ADMIN\$ only?

SecurityFocus Microsoft: RE: Any way to remove ADMIN\$ only?

<emann@questinc.o To: [focus-ms@securityfocus.com](mailto:zberkovitz@pga-inc.com)
rg> cc:

Subject: RE: Any way to remove ADMIN\$ only?

11/06/2002 08:08
AM

Could this be elaborated more on the list by others? I do not recall any conversations about the practice of which is the "best practice" or "ideal" method of setting permissions between share level and file level within the past year and a half or so that I've begun monitoring the list. Perhaps its a good time to bring the subject up?

-----Original Message-----

From: Zack Berkovitz [mailto:zberkovitz@pga-inc.com]
Sent: Tuesday, November 05, 2002 2:27 PM
To: Jim Harrison (SPG); Eric; Palumbo, Dave (Factiva);
focus-ms@securityfocus.com
Subject: RE: Any way to remove ADMIN\$ only?

The best practice is in fact to use default (Everyone=Full) share permissions and to set NTFS security on all drives (with inheritance for 2K and newer systems running NTFS 5 or greater). Share permissions should really only be used when absolutely necessary, such as on FAT volumes where ACE's cannot be applied. Conflicts between share and NTFS perms always cause headaches down the road, and NTFS perms secure the files and directories for locally logged on users as well.

If you are sharing C and D, of which one is the system drive, how will removing the admin\$ share (winnt) make the system any more secure, if the drive it resides on is shared out? NTFS permissions seem like a more comprehensive solution. The presence of any of the administrative shares is a security hole, regardless.

- Zack

-----Original Message-----

From: Jim Harrison (SPG) [mailto:jmharr@microsoft.com]
Sent: Tuesday, November 05, 2002 9:59 AM
To: Eric; Palumbo, Dave (Factiva); focus-ms@securityfocus.com
Subject: RE: Any way to remove ADMIN\$ only?

The only problem with using "net share" to create shares is that it applies default permissions to those shares it creates. These include "Everyone=Full"; obviously not an ideal scenario, especially given the default security of Windows drives (Everyone=Full). I've written a script that will create shares that only allow those accounts listed in the local server's administrator's group to have access to the share you choose to create.

RE: Any way to remove ADMIN\$ only?

SecurityFocus Microsoft: RE: Any way to remove ADMIN\$ only?

<http://isatools.org/createshare.zip>

* Jim Harrison
MCP(NT4/2K), A+, Network+
Services Platform Division

The burden of proof is not satisfied by a lack of evidence to the contrary..

-----Original Message-----

From: Eric [mailto:ews@tellurian.net]
Sent: Monday, November 04, 2002 11:55 AM
To: Palumbo, Dave (Factiva); 'focus-ms@securityfocus.com'
Subject: Re: Any way to remove ADMIN\$ only?

write a script that will launch each time upon machine bootup that 'unshares' that share.

'net share admin\$ /delete'

I don't know of any registry setting that will remove only that share and leave the others.

Understand also that anyone with admin privileges to that machine can recreate that share at any time.

At 01:11 PM 11/4/2002 -0500, Palumbo, Dave (Factiva) wrote:

>Hello,

>

>I have a scenario in which I'd like to remove the ADMIN\$ share from a
>Windows 2000 server, but keep the other default shares (c\$, d\$)
>available for an application...is there any documented/undocumented way

>to accomplish this? If this is documented, please forgive me....but I

>sure can't find it. I am aware of the

>HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters\AutoShar

>eServ

>er=0 registry key...but this disables all the default shares (save IPC\$).

>Again, I'm just looking to remove ADMIN\$.

>

>Any ideas?

>

>Thanks,

>

>Dave Palumbo

><http://pgpkeys.mit.edu:11371/pks/lookup?op=get&>

• **Previous message:** [Deus, Attonbitus: "RE: Any way to remove ADMIN\\$ only?"](#)

RE: Any way to remove ADMIN\$ only?

SecurityFocus Microsoft: RE: Any way to remove ADMIN\$ only?

- ***Maybe in reply to:*** Palumbo, Dave (Factiva): "Any way to remove ADMIN\$ only?"
- ***Next in thread:*** Jim Harrison (SPG): "RE: Any way to remove ADMIN\$ only?"
- ***Messages sorted by:*** [date] [thread] [subject] [author] [attachment]