

Forum:[Hack Forums](#)

Thread: [Disable Windows Hidden Administrative Shares](#)

Phlox - August 30, 2017, 9:55 pm

Disable Windows Hidden Administrative Shares

Administrative shares are hidden network shares created by Windows NT family of operating systems that allow system administrators to have remote access to every disk volume on a network connected system. These shares may not be permanently deleted but may be disabled. Administrative shares cannot be accessed by users without administrative privileges.

The administrative shares that have been part of Windows for a long time have been a staple for remote file management for IT pros. Administrative file shares are the hidden shares on a Windows computer with a name that ends with a dollar sign. By default, these shares share out the contents of every drive on a system and also include shares like admin\$ and IPC\$ to perform various administrative functions.

Administrative shares are a collection of automatically shared resources including the following:

Disk volumes: Every disk volume on the system is shared as an administrative share. The name of these shares consists of the drive letters of shared volume plus a dollar sign (\$). For example, a system that has volumes C, D and E has three administrative shares named C\$, D\$ or E\$. (NetBIOS is not case sensitive.)

OS folder: The folder in which Windows is installed is shared as admin\$

Fax cache: The folder in which faxed pages and cover pages are cached is shared as fax\$

IPC shares: This area, which is used for inter-process communication via named pipes and is not part of the file system, is shared as ipc\$

Printers folder: This virtual folder, which contains object that represent installed printers is shared as print\$

Domain controller shares: Windows Server family of operating system creates two domain controller-specific shares called sysvol and netlogon which do not have dollar signs (\$) appended to their names.

Note: Even if these shares were to be deleted, Windows will re-create the above shares to allow an administrator to access the drive.

To see these shares, open the Command Prompt by clicking Start Menu --> All Programs -->

Accessories, right-click on Command Prompt, and open it as an administrator. In Windows 8, 8.1 and Windows 10 simply hold down the + X keys and select the option "Command Prompt (Admin)" from the menu.

Type following command into Command Prompt and press Enter key.

Code Net Share

You see a listing similar to this:

So although the C\$, E\$, F\$ and ADMIN\$ shares are otherwise hidden, they're well known, and they represent a small security risk should an intruder get access to your network. To close this hole, you can force Windows to disable these shares with the batch script attached to this thread.

Bear in mind that some programs expect the administrative shares to be present, so disabling those shares may cause those programs to fail or generate error messages. If that happens, enable the shares by executing AutoAdminShares.bat batch script and type N letter and press Enter key to enable administrative shares.

After finish restarting your computer to put the new setting into effect, execute Net Share command again.

The output will now looks like this:

Spoiler [\(Click to View\)](#)