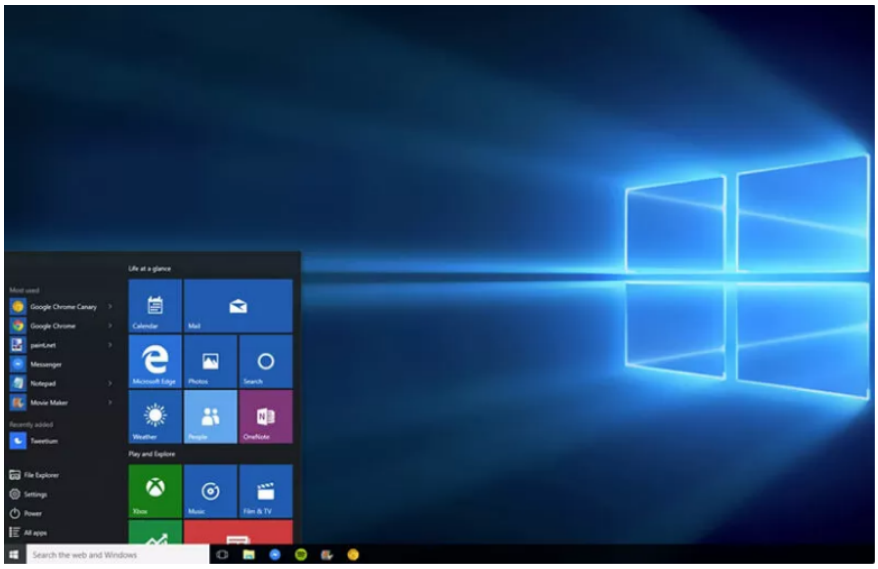
8 'tweak' Windows Group Policy any Admin should know

Windows Group Policy is a powerful tool used to configure many aspects of Windows. Most tweaking of Windows Group Policy only Admin can do. If you are an administrator of many other computers in your company or you have many other accounts on your computer, then you should take advantage of Windows Group Policy to control other users' computer usage.

Windows Group Policy is a powerful tool used to configure many aspects of Windows. Most tweaking of Windows Group Policy only Admin can do. If you are an administrator of many other computers in your company or you have many other accounts on your computer, then you should take advantage of Windows Group Policy to control other users' computer usage.



Note:

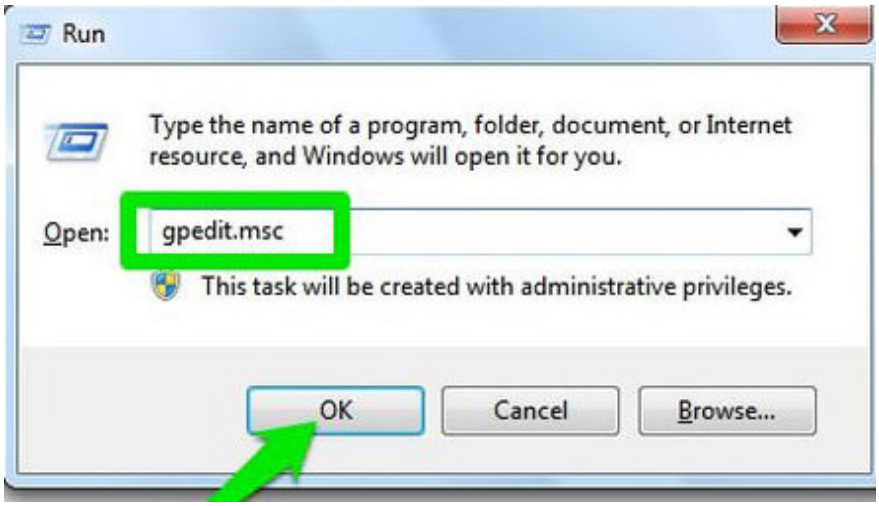
Group Policy Editor is not available on the Home version and the standard version of Windows. You must use the Professional or Enterprise version to use Group Policy.

How to access Windows Group Policy Editor?

Although there are many ways to access the **Windows Group Policy Editor** , the easiest and fastest way is to use the **Run** dialog box and this way works all versions of Windows.

To access the Windows Group Policy Editor follow the steps below:

Press the **Windows + R** key combination to open the Run command window, then type " *gpedit.msc* " into it and press **Enter** to open the Group Policy Editor.



Note that you must log in with an Admin account before accessing Group Policy. Standard accounts do not allow access to Group Policy.

1. Track account login

On Group Policy you can "force" Windows to " **record" all successful and failed logins** on your computer from any user account. You can use this information to track whether a stranger is logged in to your Windows computer.

On the Group Policy Editor window, navigate to the following link:

> **Computer Configuration => Windows Settings => Security Settings => Local Policies => Audit Policy**

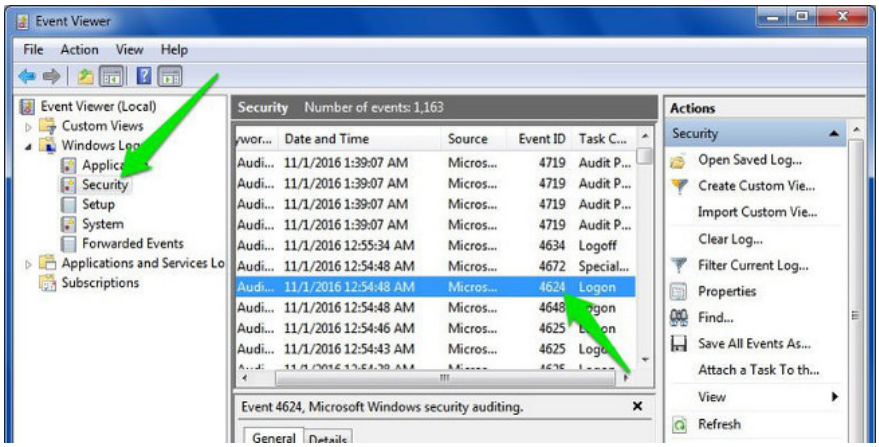
Then find and double-click on **Audit logon events** .

The Audit logon events Properties dialog box appears. Here you select **Success** and **Failure** , then click **OK** and Windows will start "recording" the log done on your computer.

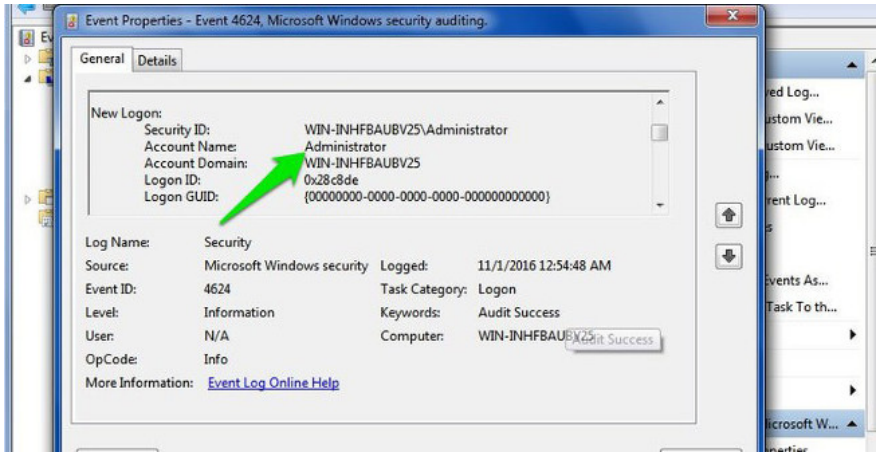
To view these logins you must access another useful Windows tool - **Windows Event Viewer** . To open Windows Event Viewer, first press the **Windows + R** key combination to open the Run command window, then enter **eventvwr** into it and press Enter.

Here you expand the **Windows Logs** section, then select the **Security** option. At the middle frame you will see all the recent events, your task is to just find the missing and successful login events on this list.

Successful logon events with *"Event ID: 4624* " and failed login are " *Event ID: 4625* ". Just search for event IDs to find login information and see the exact date and time of login.



Double click on these events to display the login account details.

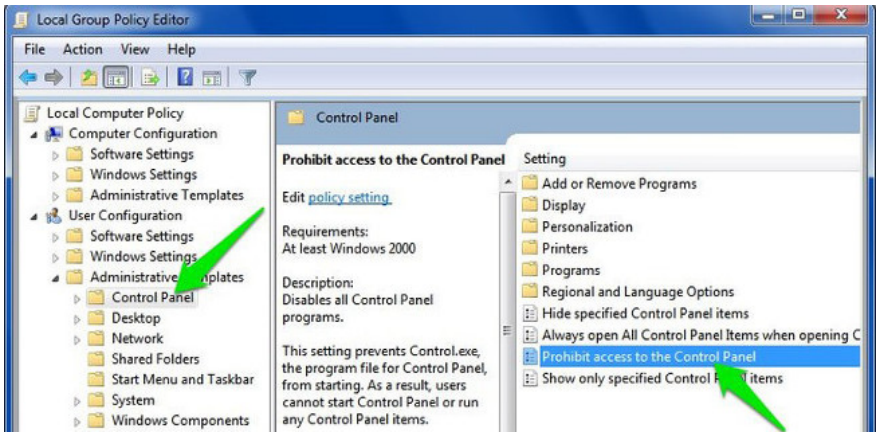


2. Block access to Control Panel

Control Panel is considered 'central' of Windows settings, including security settings and user settings. However, if you fall into the wrong hands, you will not be able to predict what will happen. To prevent possible bad situations, it is best to **block access to Control Panel** .

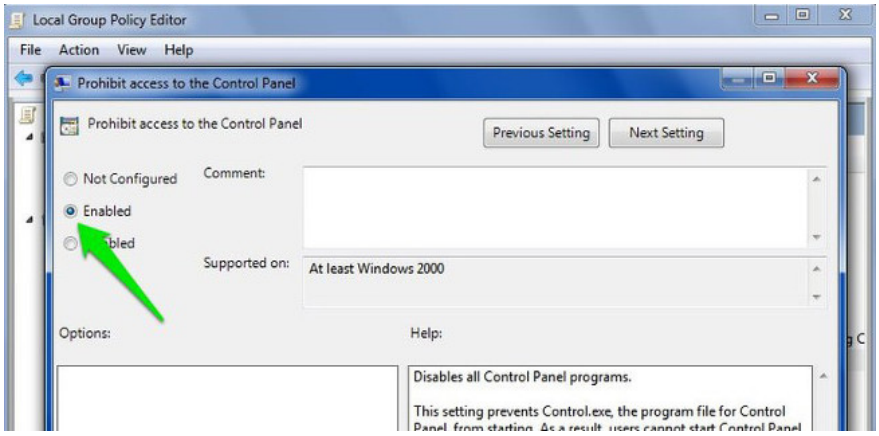
To do this, on the Group Policy Editor window, navigate to the key:

User Configuration => Administrative Templates => Control Panel



Here find and double-click the option called " **Prohibit access to the Control Panel** ".

On the Prohibit window, access to the Control Panel, click the **Enable** option to block access to the Control Panel. Now the Control Panel option will be removed from the Start Menu and no one will be able to access the Control Panel anymore, even if you open the Control Panel on the **Run** command window.



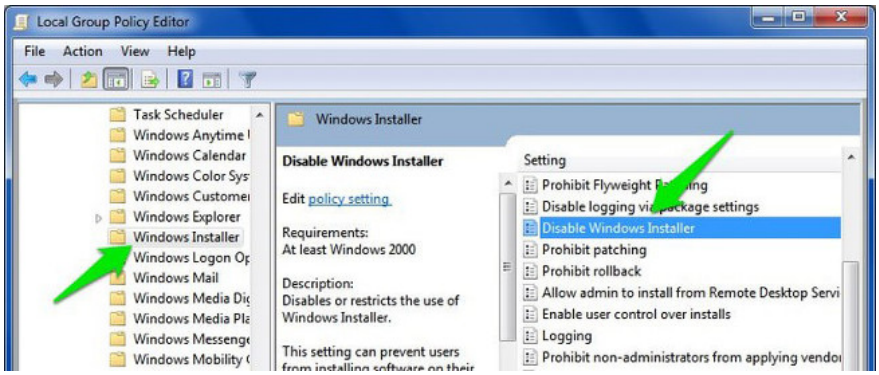
If you try to open Control Panel, an error message will appear on the screen.

3. Prevent other users from installing new software on the system

It will take a long time to "get rid of" the virus and malicious malware attacks on your computer when installing any software. Therefore, to ensure the safety of the system as well as ensure that other users illegally log in and install software and programs that are infected with malware on their computers, you should **disable the Windows installer. on Group Policy** .

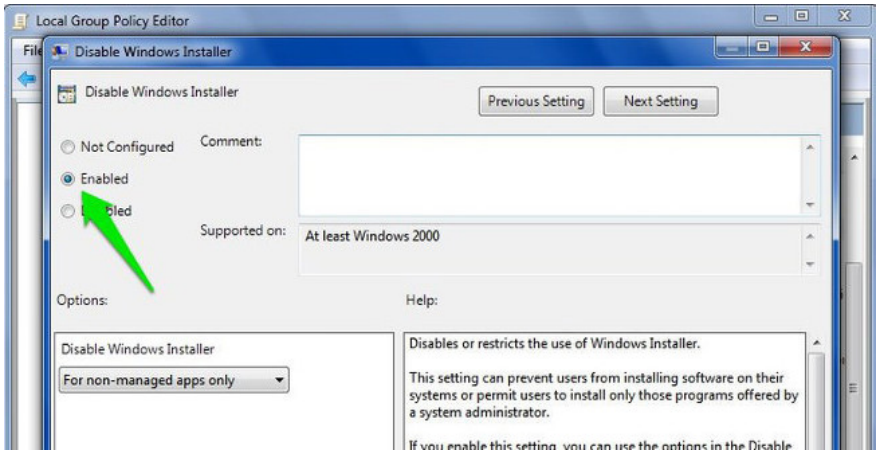
On the Group Policy window, navigate to the key:

> **Computer Configuration => Administrative Templates => Windows Components => Windows Installer**



Here find and double click on " *Disable Windows Installer* ".

On the Disable Windows Installer window, select the **Enable** option and select **Always** from the Menu dropdown in **Options** .



From now on, other users cannot install any new software on your computer, although they can download and store the application on the computer.

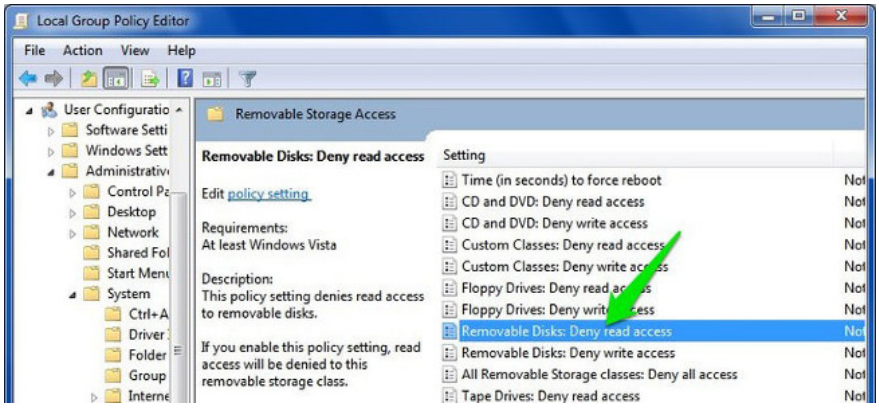
4. Disable access to removable storage devices

Mobile storage devices such as USB, or other devices are quite useful for copying and storing data, but this may also be one of the 'paths' for viruses to attack computers. friend.

If someone accidentally (or intentionally) connected a virus-infected storage device to your computer, the virus could attack your entire computer system and cause some serious problems on your computer. count.

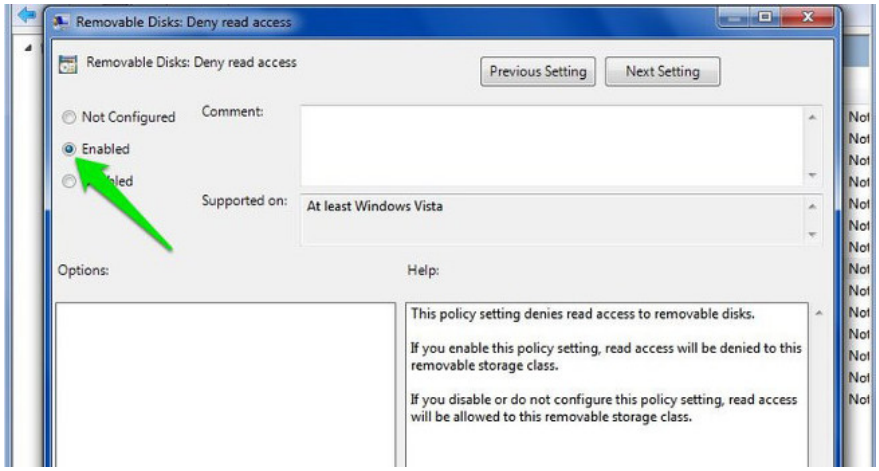
To prevent others from connecting mobile storage devices on your computer, on the Group Policy window, navigate to the key:

> **User Configuration => Administrative Templates => System> Removable Storage Access => Removable Disks: Deny read access**



Here you find and double-click " *Removable Disks: Deny read access* ".

On the Removable Disks: Deny read access window, click **Enable** to activate the option and your computer will not read any data from external storage devices (such as USB drives, etc.). Also on the Group Policy window there is an option below called " *Removable Disks: Deny write access* ". You can enable the option if you **don't want anyone to write (paste) data to an external storage device.**

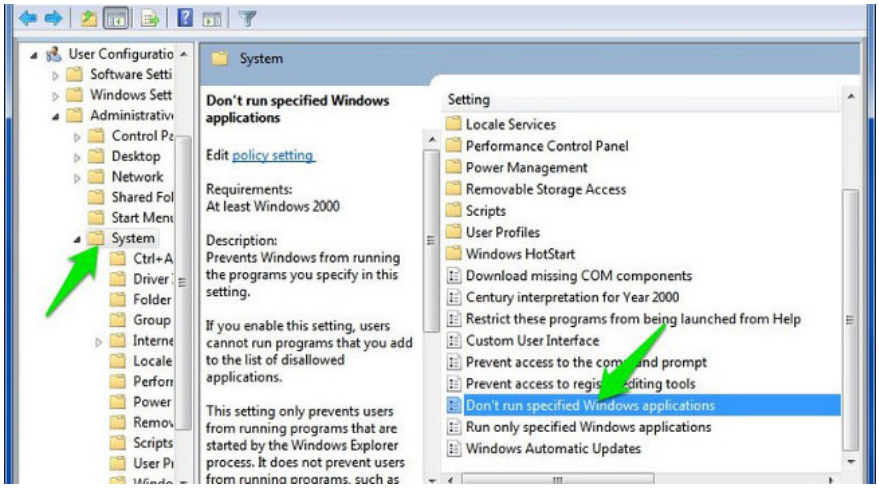


5. Prevent a specific application from running

In addition, Group Policy allows users to create a list of applications to **prevent the operation of these applications.**

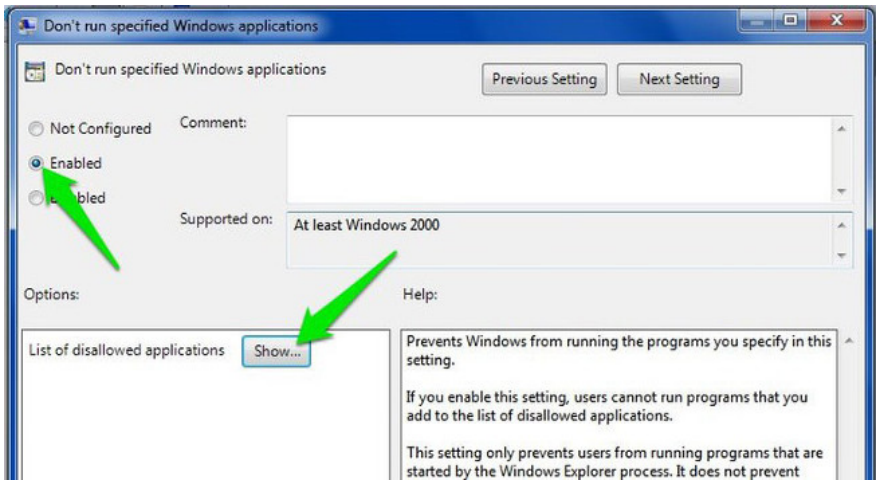
To do this, on the Group Policy window, navigate to the key:

> **User Configuration => Administrative Templates => System => Don't run specified applications Windows**



Here you find and open the " *Don't run specified Windows applications* " option.

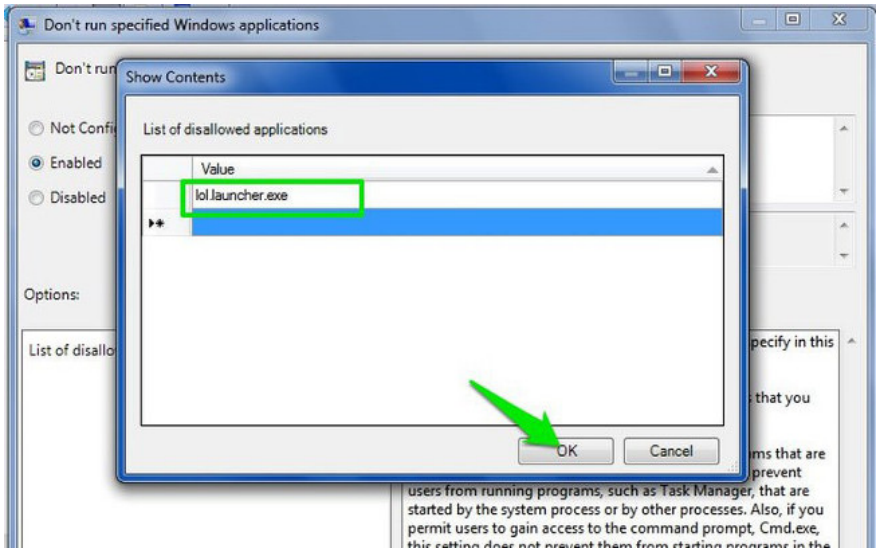
On the Don't run specified Windows applications window, click **Enable** to activate the option and click **Show** to start the process of creating a list of applications that you want to block.



To create a list, you must enter the executable name of the .exe application to be able to block the application, such as **CCleaner.exe** , CleanMem.exe or lol.launcher.exe.

The best way to find the exact executable name of the application is to find the application folder on Windows File Explorer, then copy the executable name of the program correctly (with the extension ".exe").

Enter the executable name in the list and click **OK** to start the application blocking process.



Also on the Group Policy window there is the option to **Run only specified Windows applications** . If you want to disable all types of applications, except for some important applications, you can use the option to create

a list of applications that you want to block.

6. Disable Command Prompt and Windows Registry Editor

Command Prompt on Windows allows you to enter commands to the computer to execute that command and access the system. However, hackers can use the Command Prompt (CMD) to gain unauthorized access to sensitive data.

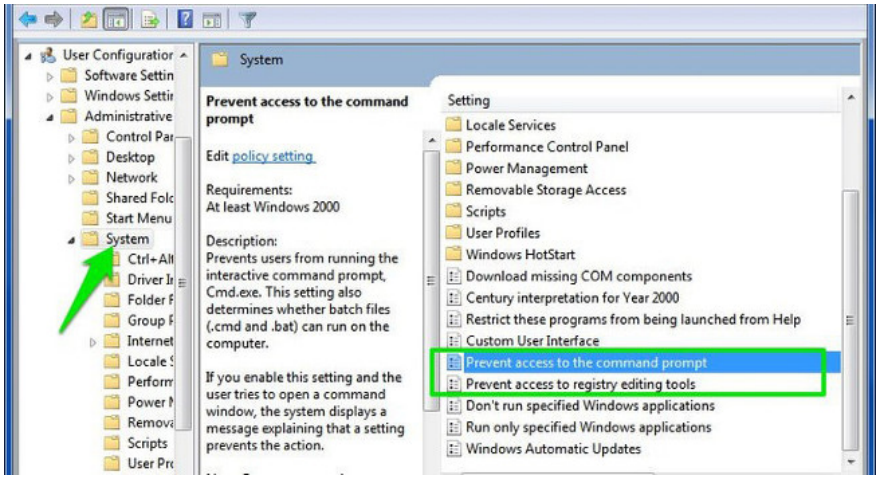
Both Command Prompt and Windows Registry Editor are tools that can **disable all activities on Windows computers, especially Windows Registry Editor** .

If you want to ensure safety and security issues on your computer, you should disable the Command Prompt and the Windows Registry Editor.

To do this, on the Group Policy window, navigate to the path:

User Configuration => Administrative Templates => System

Here you can find and double-click the options called " *Prevent access to the command prompt* " and " *Prevent access to registry editing tools* ". Then on the Prevent access to the command prompt window and the Prevent access to registry editing tools window, click **Disable** to disable these options.



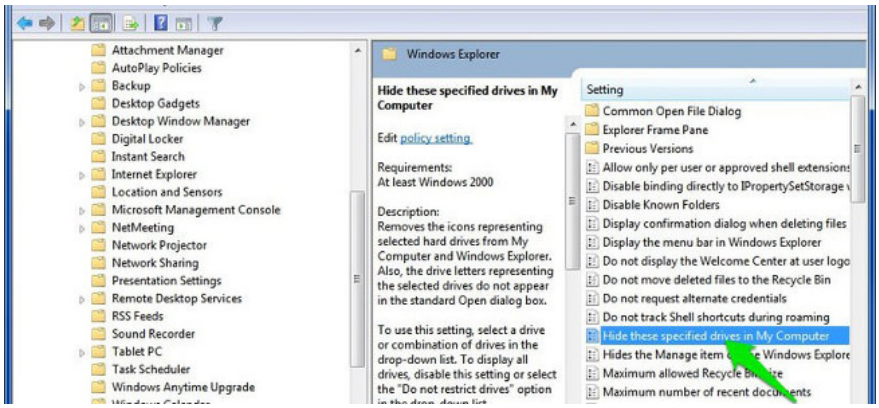
From now on, other users cannot access Command Prompt and Registry Editor anymore.

7. Hide drive partitions from My Computer

If a specific drive on your computer contains sensitive data and you don't want other users to access and steal that data, then you can **hide it from My Computer** and the person. Other users cannot find them.

To do this, on the Group Policy window, navigate to the path:

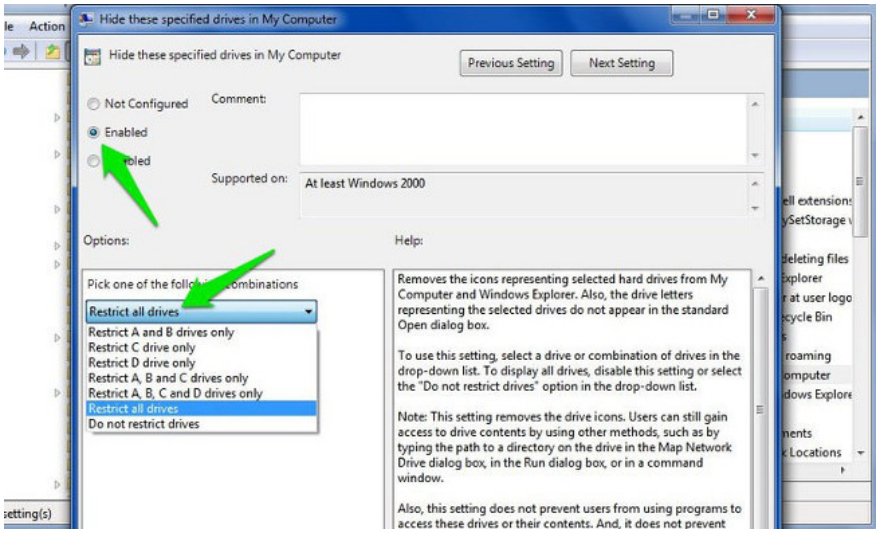
User Configuration => Administrative Templates => Windows Components => Windows Explorer => Hide these specified drives in My Computer



Find and double-click the option named " *Hide these specified drives in My Computer* ".

On the window Hide these specified drives in My Computer click Enable to enable the option.

After activating the option, from the **Options** dropdown **menu** , select the drive you want to hide. Finally click **OK** to hide the drive on the system.



8. Tweak Start Menu and Taskbar

Group Policy gives you dozens of tweaks for Start Menu and Taskbar according to your preferences. These tweaks are available for both Admin and regular users.

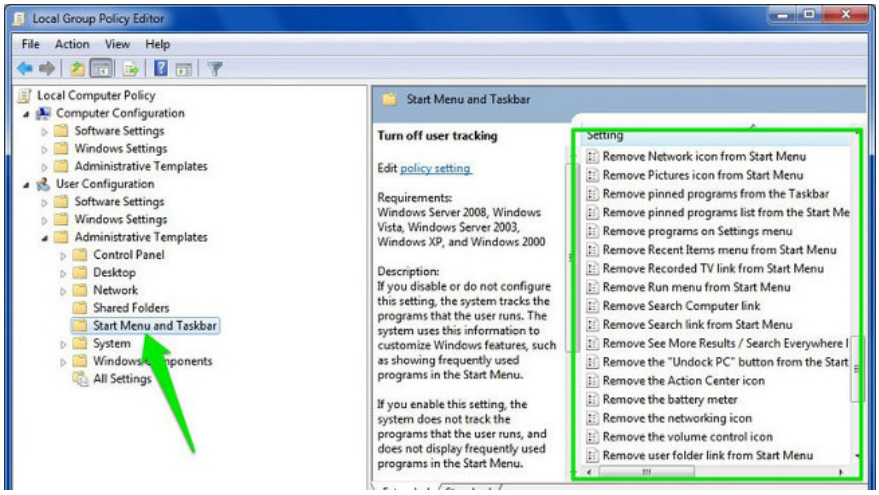
To tweak Start Menu and Taskbar, on the Group Policy Editor window you navigate by the path:

User Configuration => Administrative Templates => Start Menu and Taskbar

Here you will find all the tweaks along with explanations.

The tweaks are quite easy to understand. Besides Windows also provides detailed descriptions for each tweak.

You can do some things like change the Power button function on the Start Menu, prevent users from pinning the program on the Taskbar, restrict the search to the Search option, hide system tray notifications, hide icons battery, prevent changing the Taskbar and set up the Start Menu, prevent users from using the Power options (shutdown, hibernate (hibernate), .), remove the **Run** option from Start Menu, .



Refer to some of the following articles:

1. Remove root malware (malware) on Windows 10 computers

1. Instructions for activating and customizing virtual Touchpad on Windows 10

1. How to enable or disable SuperFetch on Windows 10/8/7?

Good luck!

You finished reading the article "**8 'tweak' Windows Group Policy any Admin should know**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.