

Method 1: How to Prevent Specific Users from Accessing a Drive or Folder.

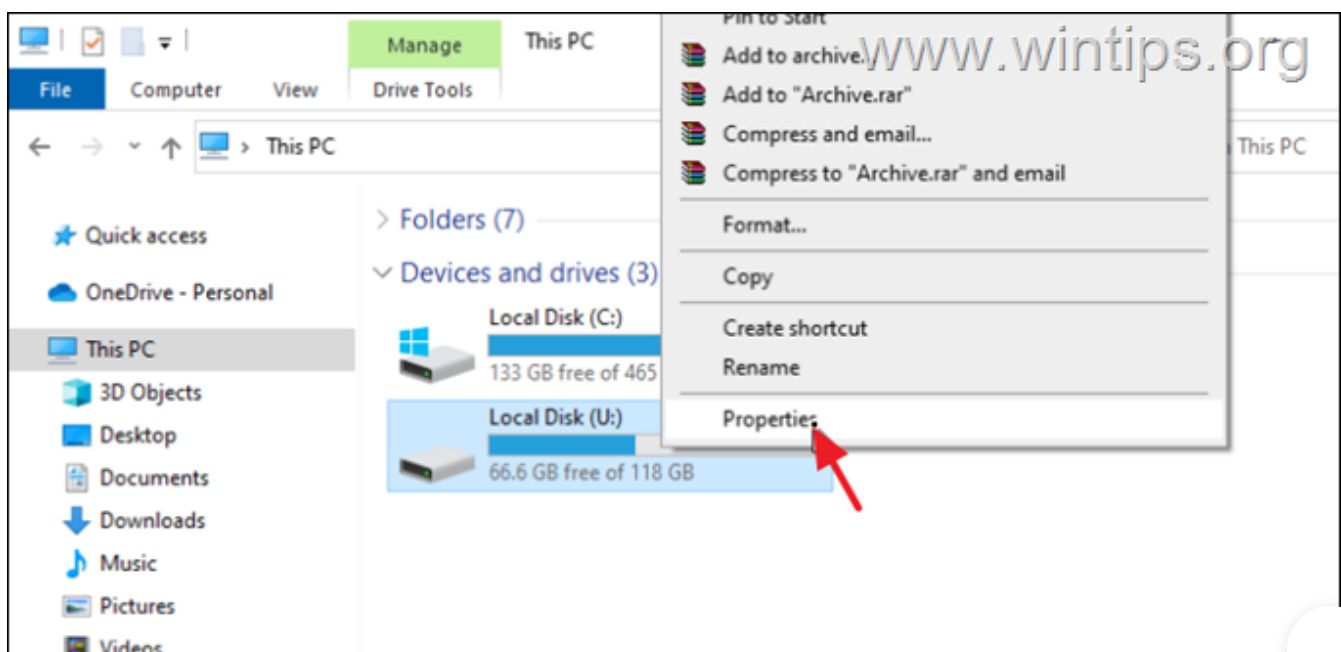
The first and best method* to deny access to a drive/folder is to change the user permissions on the drive/folder properties.

* **Note:** This is the best method, because it allows you to prevent only specific users from accessing the contents of a disk unit or a folder. All other methods listed here prevent access to all users (including you).

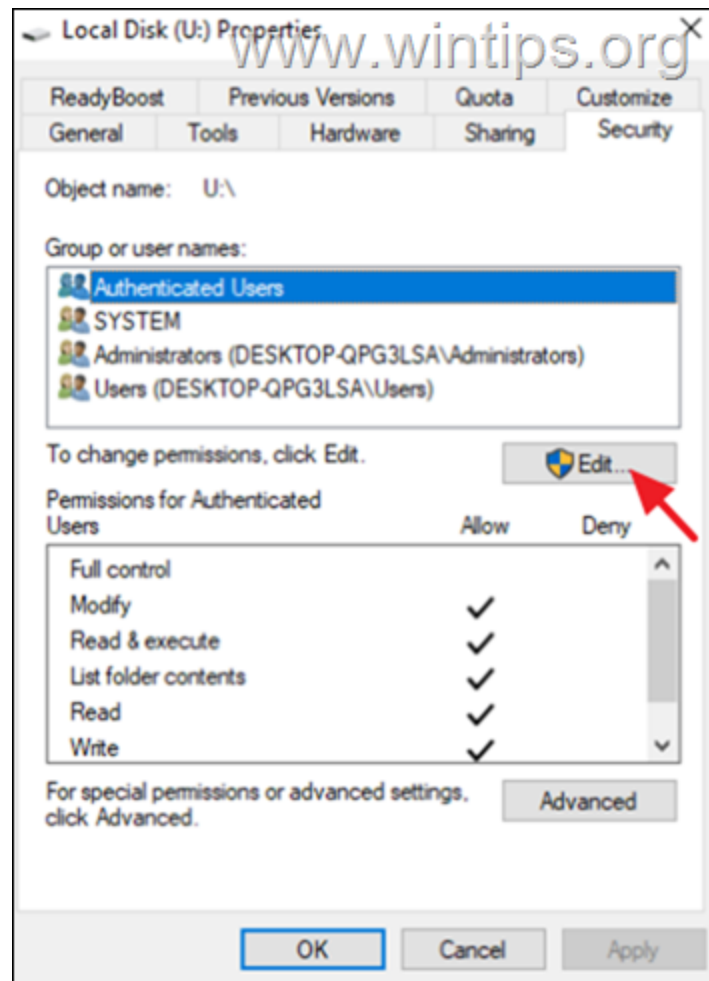
To disallow certain users to access the contents of a folder/drive:

AD

1. In File Explorer, **right-click** the drive on which you want to deny access to specific users, and then click **Properties**.

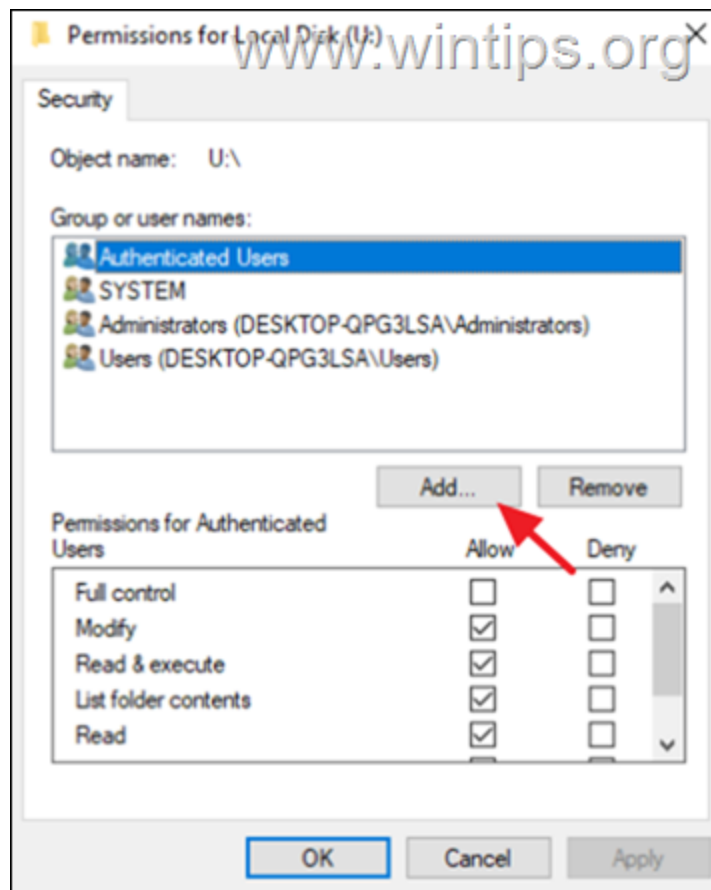


2. Select the **Security** tab, then click the **Edit** button.



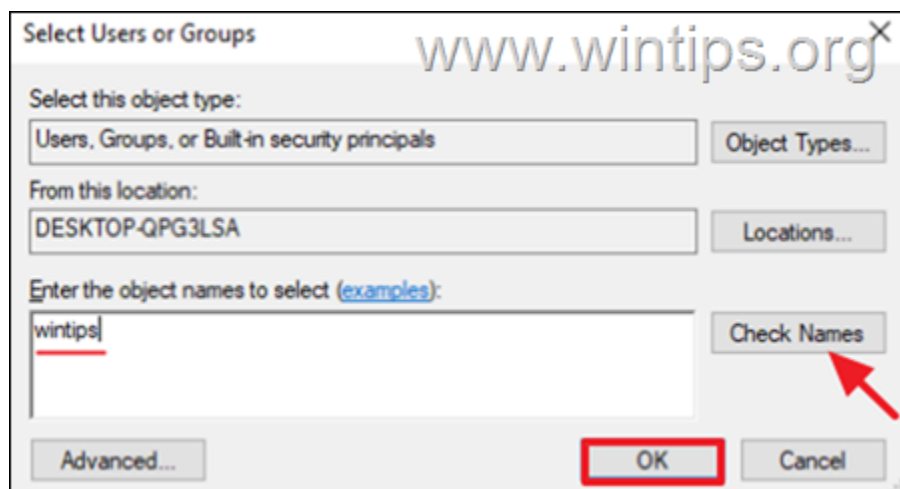
AD

3. Click **Add** to select the user you want to prevent from accessing your drive.

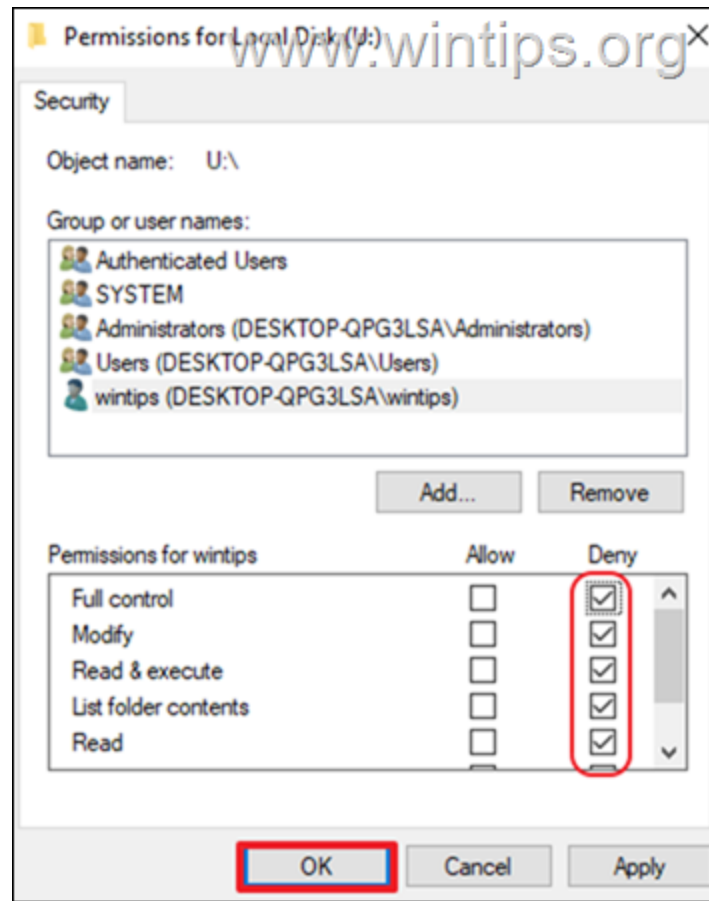


4. **Type** the **username*** of the user you want to restrict access to, and to confirm, click **Check Names**. Then select **OK**. *

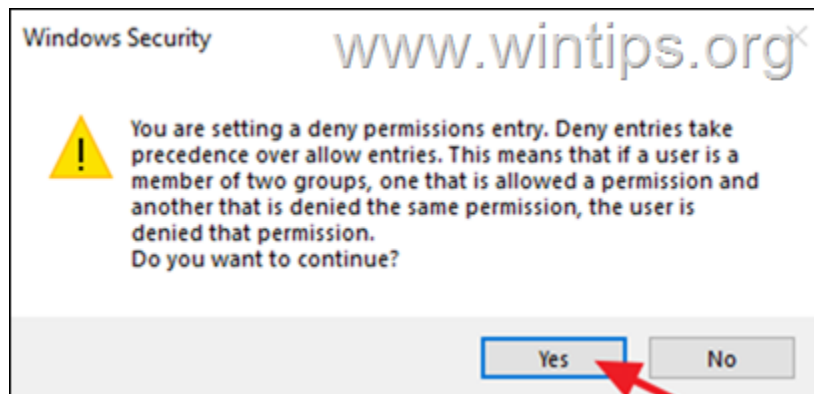
* **Note:** You need to know the correct username of the account you want to restrict. An easy way to view the users on your pc, is to view the names of the profile folders under the "C:\Users\" folder.



5. Now in **Permissions for local disk window**, select the user you just added and in the **Permissions** section, tick **Deny**, restricting access for **Full control**. Now select **Apply >> OK**.



6. Click **Yes** when prompted to apply the permissions and then close all windows.




7. At this point, you have successfully prevented a specific user from accessing the selected drive. If you want to restrict access to more users, follow the same steps above.

Method 2. How to Prevent Access to Local Drive to All Users in Registry.

The next method to prevent users to access a local drive in Windows 10, is by using Registry. *

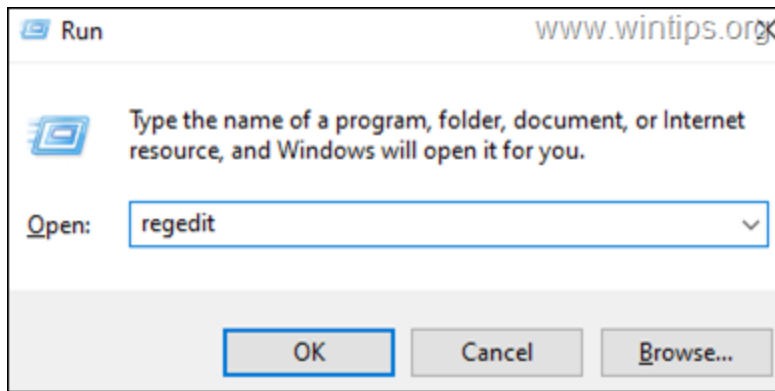
* **Note:** Use this method only if you want to prevent the access to all users (including you).

Important: Making incorrect changes to the Registry can cause serious damage to your device and could require you to reinstall Windows. Therefore, be careful when making changes to the Registry Editor and always back up the Registry before making any changes.

1. Press the **Windows**  and **R** keys to open the **Run** command box.
2. Type **regedit** and hit **Enter**: *

* **Note:** If you see a User Access Control (UAC) warning window asking for permission, click on **Yes**.





3. In Registry Editor, navigate to the following path:

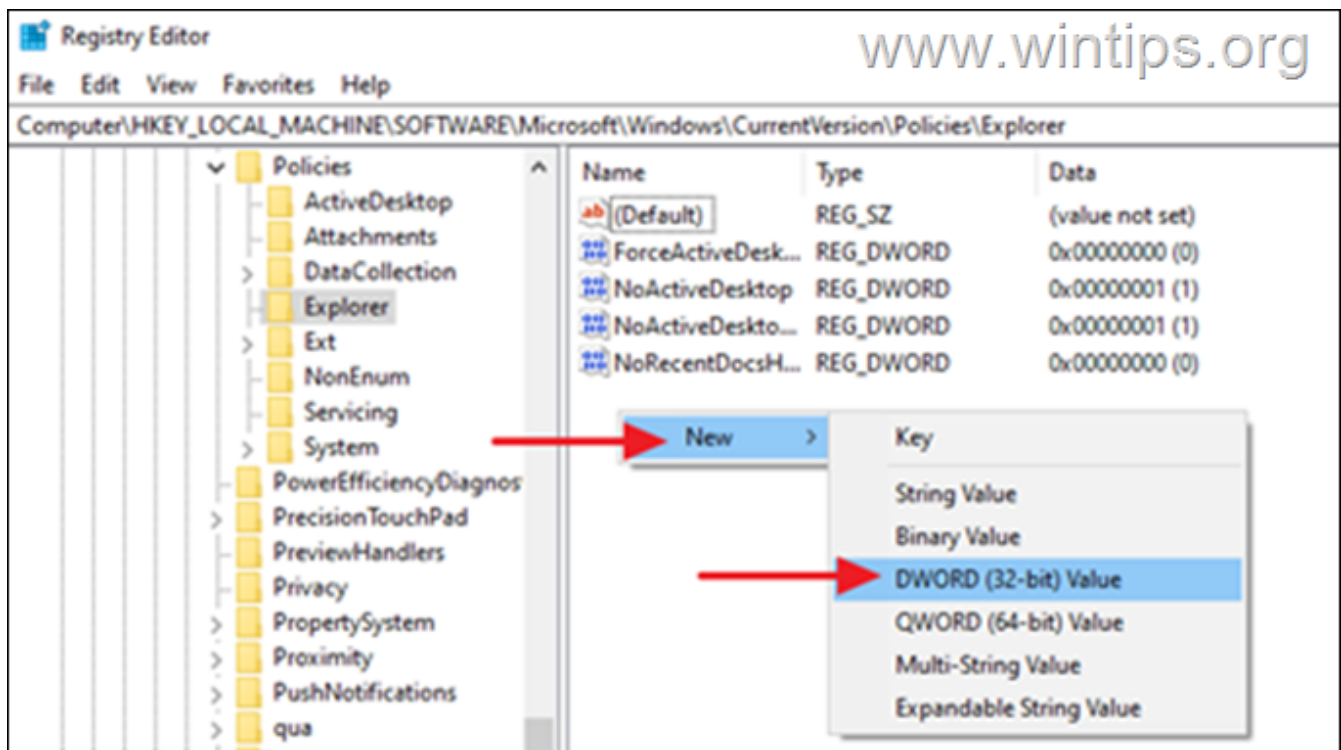
AD

1. Navigate to the following path on Registry Editor:

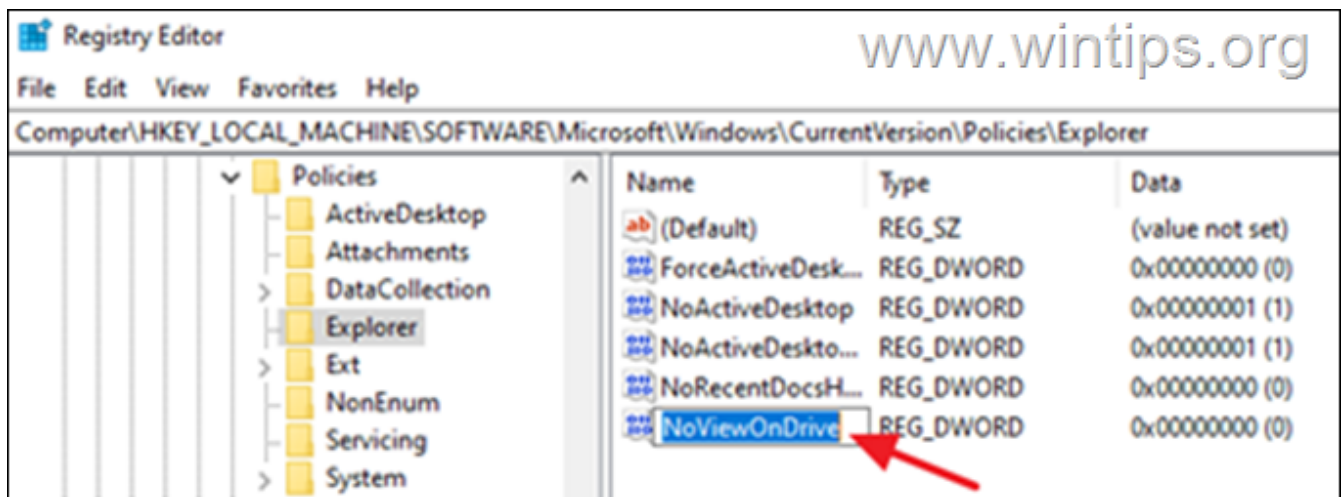
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

4. **Right-click** at the blank space on the right side and select **New > DWORD (32-bit) Value**.





3. Type **NoViewOnDrive** as the name of the new DWORD, then press **Enter**.

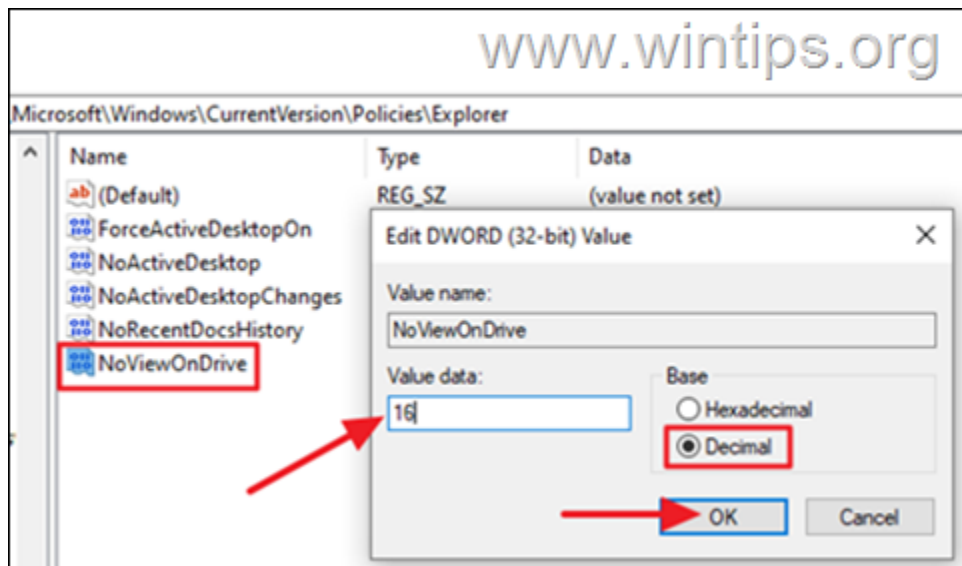


AD

4a. Double-click at the newly created **NoViewOnDrive** value, and select **Decimal** at the Base options.

4b. Now change the value data to the number corresponding to the drive letter, according to the table below and press **OK**.*

e.g To hide the drive "E:" with have to type "16" in the Value Data box.



* **Note:** See the table below to find the value data for each drive letter.

Drive letter	Value Data	Drive Letter	Value Data
A	1	N	8192
B	2	O	16384
C	4	P	32768
D	8	Q	65536
E	16	R	131072
F	32	S	262144
G	64	T	524288
H	128	U	1048576
I	256	V	2097152

J	512	W	4194304
K	1024	X	8388608
L	2048	Y	16777216
M	4096	Z	33554432

AD

5. When done, **close** the registry editor and **restart** your PC to apply the change.

6. After restarting every user who tries to access the drive will receive the error:

“This operation has been canceled due to restrictions in effect on this computer. Please contact your system administrator.”

* **Note:** To remove the access restriction, open the registry editor again and **delete** the **NoViewOnDrive** DWORD Value from the above mentioned registry location and **restart** your PC.

Method 3: How to Deny Access to a local drive using Group Policy.

Alternatively, local group policy is also effective for restricting users to access a local drive. Compare to Registry Editor, group policy has a limited amount of drive letters that can be restricted.


* **Notes:**

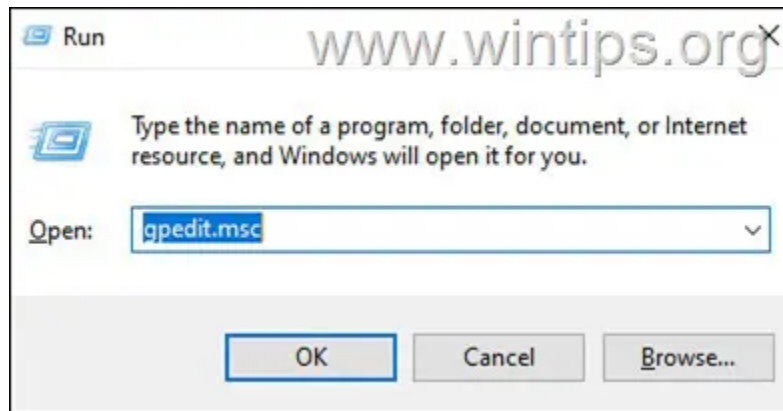
1. To use Group Policy method, you must be running Windows 10

Pro/Enterprise/Education edition. Local group policy is not available on Windows 10 Home.



2. Use this method only if you want to prevent the access to all users (including you).

1. Simultaneously press the **Windows**  + **R** keys to open the Run command box.
2. In the text field of the dialog box, type **gpedit.msc** and hit **Enter** to open the Group Policy Editor.



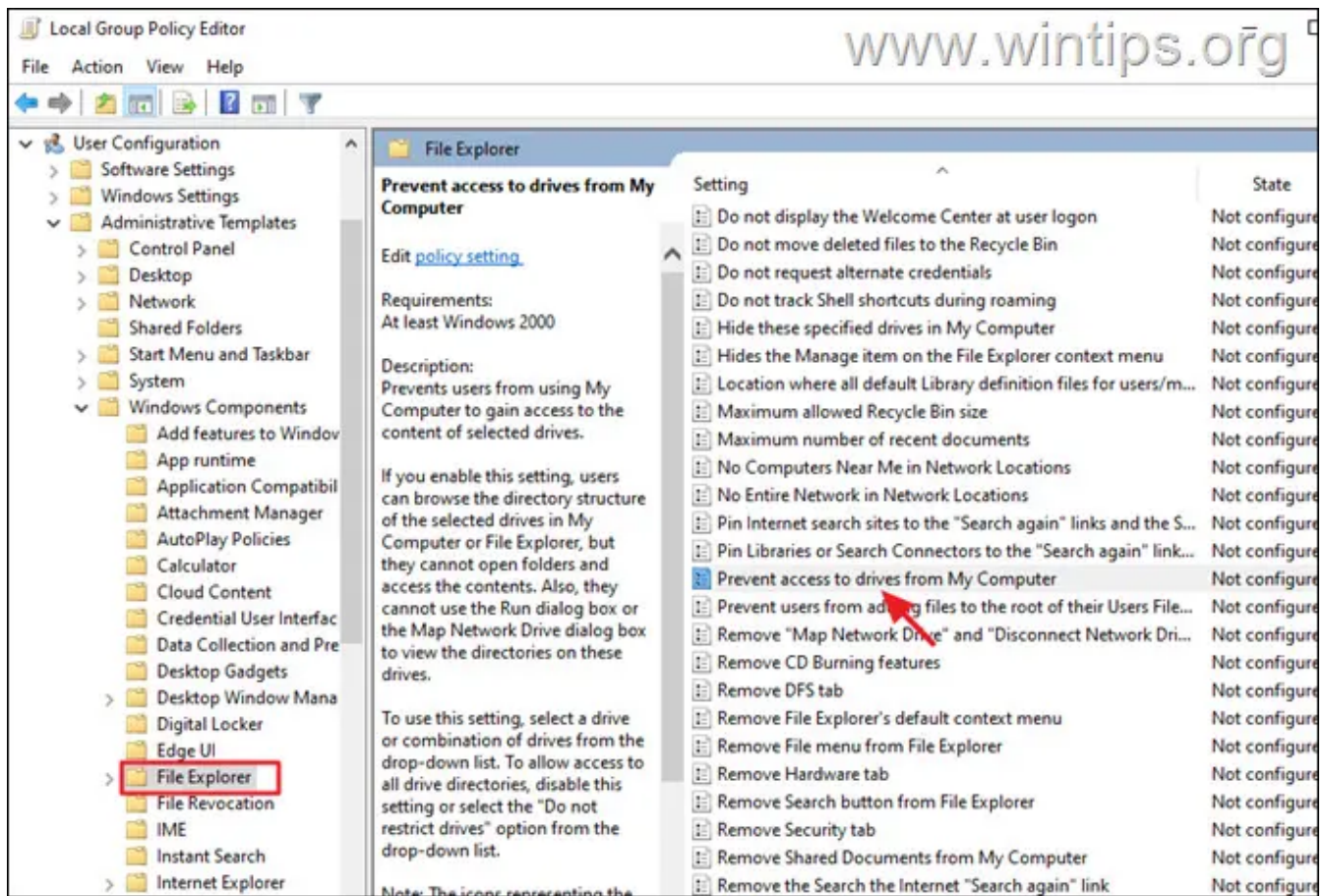
AD

3. Navigate to the following path in the Group Policy Editor.

- **User Configuration → Administrative Templates → Windows Components → File Explorer**

4. At the right side **double-click** to open the **Prevent Access to drives from My Computer** policy.*

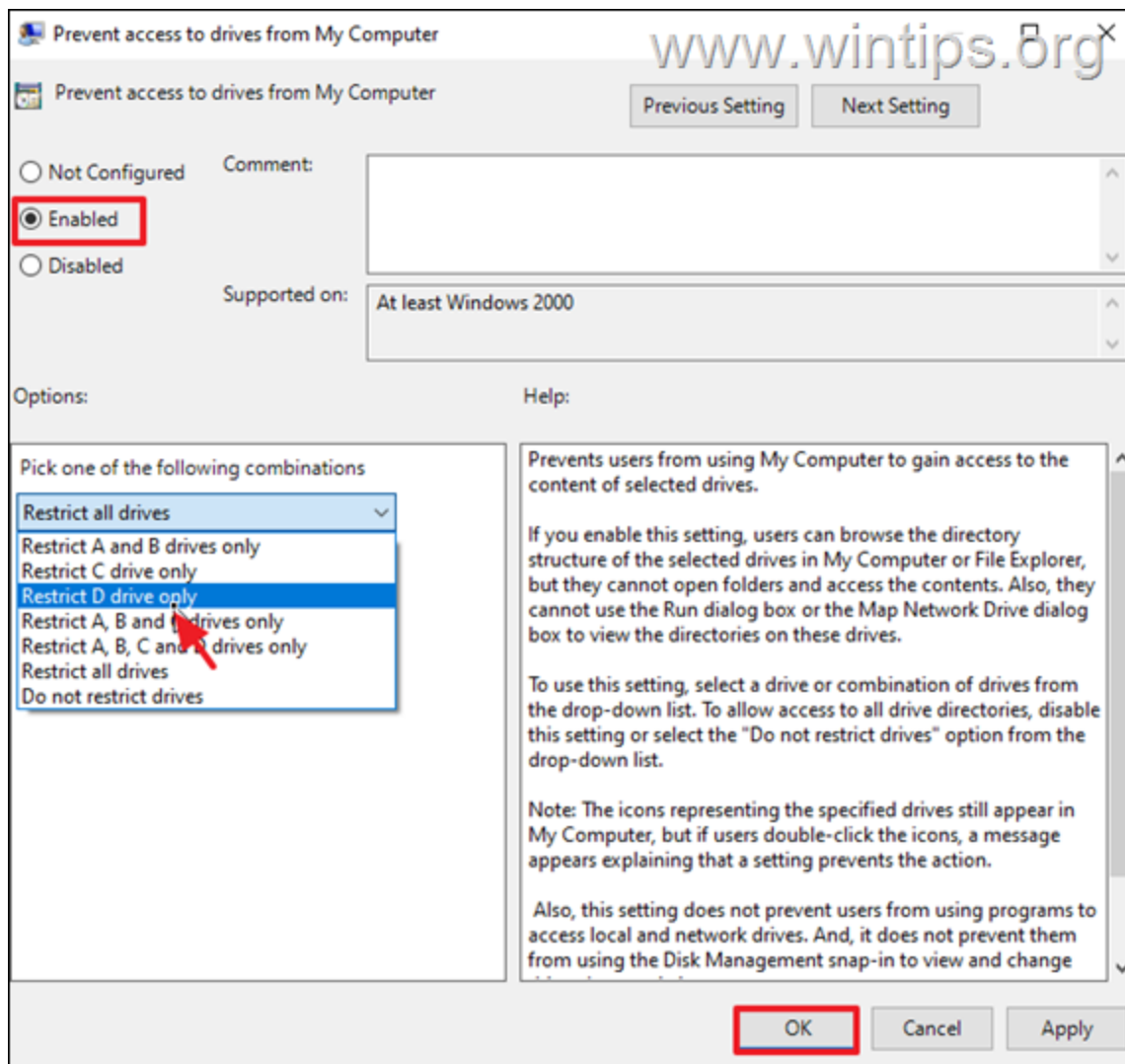
* **Info:** This policy prevents users from using My Computer to gain access to the content of selected drives. If you enable this setting, users can browse the directory structure of the selected drives in My Computer or File Explorer, but they cannot open folders and access the contents. Also, they cannot use the Run dialog box or the Map Network Drive dialog box to view the directories on these drives.



AD

4. At the new window that will pop up, select **Enabled** and from the dropdown menu below **Options**, select the drive letter* you want to hide. When done, click **Apply** and **OK**.

* **Note:** If you don't see the drive letter that you want to hide, then use one of the above methods, because group policy doesn't allow to hide all drives/letters. (Yes, this another good job from MS!)



5. Close the Group Policy Editor.

6. Now, check in File Explorer to verify that you no longer have access to the drive with error:*

A

"This operation has been canceled due to restrictions in effect on this computer. Please contact your system administrator."