Deny All Access to Removable Devices or Media

By Archiveddocs

Archived: 2026-04-02 12:32:42 UTC

Applies To: Windows Server 2008

You can use this procedure to restrict the ability of your users to both read and write to or from any removable device that falls into the following categories:

- **CD and DVD drives**. This type of drive uses removable media.
- **Floppy disk drives**. This type of drive uses removable media.
- **Removable drives**. This type of drive is an external drive connected to the computer using a USB or IEEE 1394 connection. It includes both hard disk drives and flash memory drives.
- **Tape drives**. This type of drive uses removable media.
- **Windows Portable Devices**. This type of device includes media players, smart phones, and so on.

Membership in the local **Administrators** group, or equivalent, is the minimum required to complete this procedure.

To deny all access to removable devices

1. Open the Group Policy Management Editor. To do so, click **Start**, and then in the **Start Search** box, type `mmc gpedit.msc`.
2. In the navigation pane, open **Local Computer Policy**. Then do one of the following:
    - If you want the policy to affect all users on the computer, open **Computer Configuration** in the navigation pane.
    - If you want the policy to affect only the currently logged on user, open **User Configuration** in the navigation pane.
3. Continue by opening the following folders: **Administrative Templates**, **System**, and **Removable Storage Access**.
4. In the details pane, double-click **All Removable Storage classes: Deny all access**.
5. Click **Enabled.**
6. Click **OK** to save your changes.

Additional considerations

- If the device to which you wish to prevent access is not covered by any of the other categories, you can deny read and/or write access to devices that have a specified device setup class GUID. See the second procedure in Control Read or Write Access to Removable Devices or Media to create a list of device setup class GUIDs for devices that you do not want users to read to or write from.
- If a device affected by this policy is currently in use, you might have to restart the computer to enforce the policy immediately. See Force a Restart to Ensure Removable Storage Access Policy is Enforced.
- If you edit policy settings locally on a computer, you will affect the settings on only that one computer. If you configure the settings in a Group Policy object (GPO) hosted in an Active Directory domain, then the settings apply to all computers that are subject to that GPO. For more information about Group Policy in an Active Directory domain, see Group Policy (https://go.microsoft.com/fwlink/?LinkId=55625).
- Make sure to test all applications required by the users that will be affected by this policy setting to ensure that you do not prevent applications required by the user from working properly.
