REMOVABLE STORAGE AND SYSTEM SECURITY IN WINDOWS 7

Security Issues

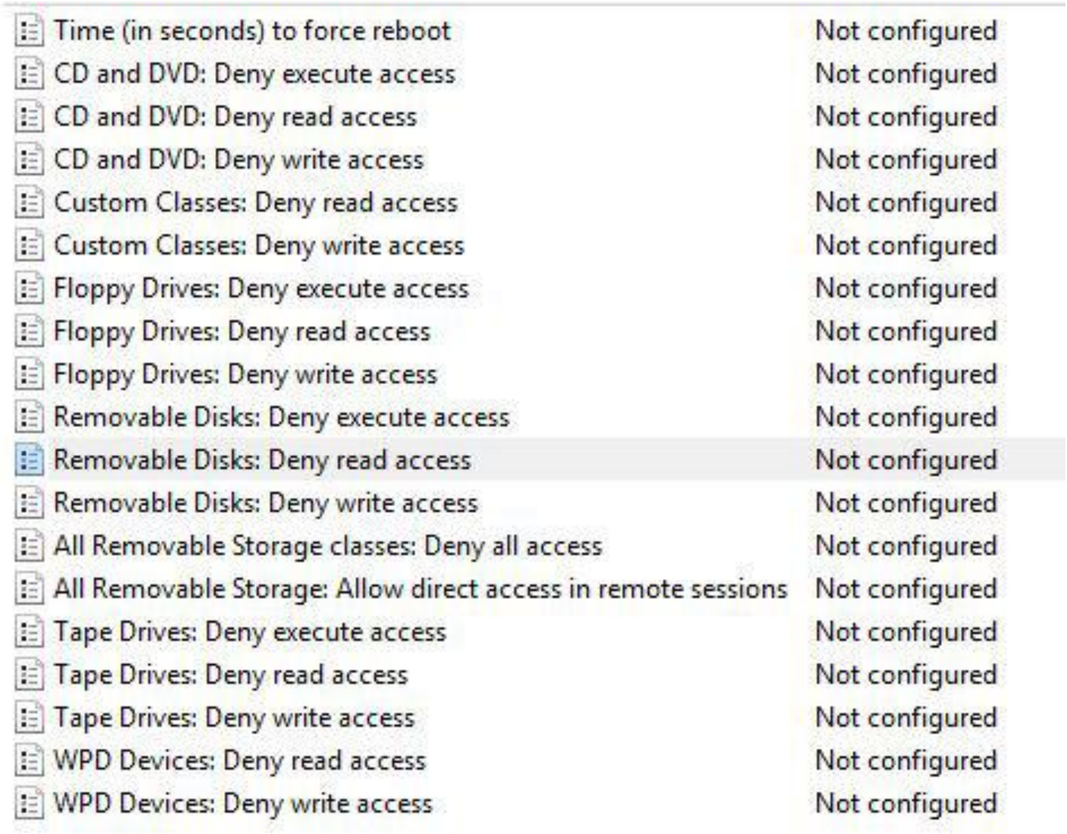
Removable devices actually represent a big security risk because they can be used to easily copy sensitive data to it (to steal personal or confidential data). To deal with this problem we can use **Removable Storage Access** policies in Group Policy. For example, we can forbid writing of data to removable media. We can also prevent users from running software from removable media, or to copy data from the removable media to our computer.

Group Policies related to hardware depend on the type of device. For example, we can set restrictions on our CDs, DVDs, floppy drive, removable disks. We can also set custom class restrictions which are based on Globally Unique Identifier (GUID). A GUID is a 16-byte alphanumeric string specific to a device. We can also restrict all removable storage at once.

We can deny read, write and execute actions on our removable devices. This also includes our mobile phones, media players and similar devices (for this we use **Windows Portable Devices (WPD) policies**).

To enforce configured policies we can set the time to force reboot. If we don't configure this setting, policies will not be take effect until the system is restarted.

To open Group Policy we can enter gpedit.msc in Search box. Removable Storage Access policies can be set on the whole system or per-user basis. In our example we will forbid users to read and write to removable disks. To do that we will go to **Computer Configuration > Administrative Templates > System > Removable Storage Access**.



Time (in seconds) to force reboot	Not configured
CD and DVD: Deny execute access	Not configured
CD and DVD: Deny read access	Not configured
CD and DVD: Deny write access	Not configured
Custom Classes: Deny read access	Not configured
Custom Classes: Deny write access	Not configured
Floppy Drives: Deny execute access	Not configured
Floppy Drives: Deny read access	Not configured
Floppy Drives: Deny write access	Not configured
Removable Disks: Deny execute access	Not configured
Removable Disks: Deny read access	Not configured
Removable Disks: Deny write access	Not configured
All Removable Storage classes: Deny all access	Not configured
All Removable Storage: Allow direct access in remote sessions	Not configured
Tape Drives: Deny execute access	Not configured
Tape Drives: Deny read access	Not configured
Tape Drives: Deny write access	Not configured
WPD Devices: Deny read access	Not configured
WPD Devices: Deny write access	Not configured

Removable Storage Policies

In this window we will enable the following policies: "Removable Disks: Deny read access" and "Removable Disks: Deny write access". Those policies will be active when the system reboots. We can also force the reboot by using the "Time (in seconds) to force reboot" policy. Settings for users are available in **User Configuration > Administrative Templates > System > Removable Storage Access**.

Source: http://www.utilizewindows.com/7/management/397-removable-storage-and-system-security-in-windows-7