

## Installation instructions for the current version of USB Drive Guard

[www.usbdriveguard.com](http://www.usbdriveguard.com)

Contact Email: [support@usbdriveguard.com](mailto:support@usbdriveguard.com)

Default User Name: admin

Default Password: admin

**Usage:** To remove and prevent the usage of unauthorized USB storage devices and optical disk drives.

### Requirements:

32 Bit or 64 Bit versions of the following versions of Windows: XP, Windows 2000, Windows 2000 Server, Windows 2003 Server, Windows 2008 Server, Windows Vista, Windows 7.

You can download the newest version from the website [www.usbdriveguard.com](http://www.usbdriveguard.com) at anytime. Updates are issued as needed. If you have any suggestions for USB Drive Guard please email us at [support@usbdriveguard.com](mailto:support@usbdriveguard.com).

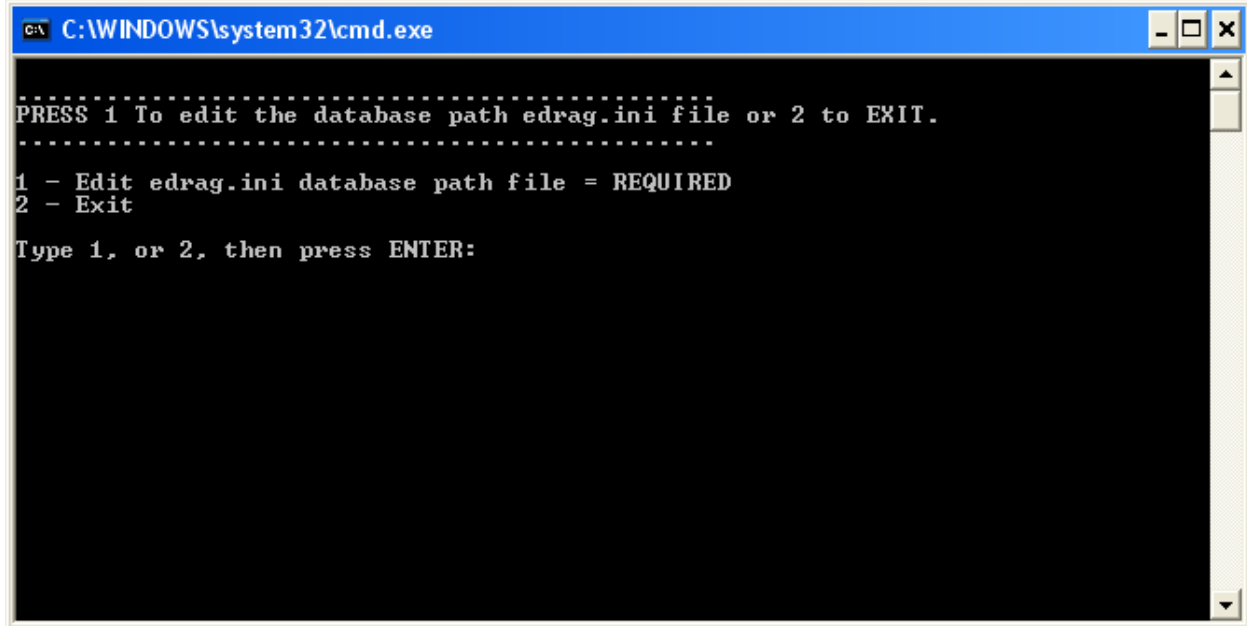
### Installation Steps:

The file USBsetup.exe is used to install either the Server or Client installs.

**Server Installation:** Start the application USBsetup.exe you just downloaded and choose Server Setup Installation. You will install the Server Setup Installation onto just **one** PC on your network. Give everyone read and write access to this installation folder, and subfolders. The default installation path is "C:\USBDRIVEGUARD". All computer users running the USB ejection client will need to read and write to this folder and subfolders. You do not have to install on a version of Windows "Server". Any version of Windows from Windows 2000 and newer will do for the Administrator Server application. You can create a shortcut for the main Administrator application file called "USBAdmin.exe" and place this shortcut onto any computer on your network to use this application.

The default user name and password when logging into the USB Drive Guard Administrator is "admin" for both. You should change the password as soon as you can for security purposes.

**Work Station Client Installation:** Start the application USBsetup.exe you just downloaded and choose Client Setup Installation. This type of install is for every computer on your network that you want to run the USB Drive Guard Client on. Do not change the default installation path. This client application needs 32 Bit or 64 Bit versions of the following versions of Windows: XP Professional or XP Home Edition, Windows 2000, Windows 2000 Server, Windows 2003 Server, Windows 2008 Server, Windows Vista, Windows 7. Restart the PC after installing the client application. At the end of the installation you will see the following console window.



```
C:\WINDOWS\system32\cmd.exe
.....
PRESS 1 To edit the database path edrag.ini file or 2 to EXIT.
.....
1 - Edit edrag.ini database path file = REQUIRED
2 - Exit
Type 1, or 2, then press ENTER:
```

Enter 1 to edit the ini file that was just installed. This ini file is the direct network path to the shared database installation folder on the main computer on your network that you shared with full read and write rights in step 1.

**IMPORTANT: edrag.ini edit instructions. Work Station Client Installation Only.**

The content of the edrag.ini is the network, or local path to the folder that has the database files and subfolders that you setup in step one. The sample edrag.ini file that came with this installation has the following text "\\ServerComputerName\USBDRIVEGUARD". When you edit the edrag.ini file, you will need to meet your specific network naming requirements. Do one of the following;

- **Example 1. (Recommended) Database files are located on a server on your network.** If the server has a computer name of "YOURFILESERVERPC" and on this server you have shared and installed the ADMIN install to a folder called "USBDRIVEGUARD" then you would edit the edrag.ini file with only the following on the first line "\\YOURFILESERVERPC\USBDRIVEGUARD" without the quotes and without any spaces and all on the first line. You do NOT need a dedicated PC for the USB Drive Guard Administrator, just a decent PC running at least Windows 2000 on your network will do. Make sure to give all users full read and write access to this folder and subfolders.
- **Example 2. Database files are located on the local PC.** If you are not networking this application, and this is a single computer setup then use the following example. If the "C" drive on the root of this computer you has a folder called "C:\USBDRIVEGUARD" your edrag.ini file will be the following "C:\USBDRIVEGUARD" without the quotes, without any spaces, and all on the first line. This type of setup is NOT for a network, and only for single PC use. Network setup use example 1.

In the startup folder the client application called "garde.exe" will be placed so that each time a user logs in the application will start. The "garde.exe" file can be renamed to whatever you want as long as it keeps the ".exe" at the end of the file name.

## **This concludes the installation instructions.**

### **Read Notes:**

1. USB Drive Guard will never try to remove a drive with a drive letter A, C. Drives "A" are usually a floppy, and the C drive of course is the main fixed disk.
2. Internal fixed hard drives that have a drive letter of D or greater will try to be removed, but since they are a fixed disk it will not eject and it will fail, but will notify the user and log the ejection. If there is more than one fixed drive inside the PC, or you have a drive that is partitioned you need to add each of them to the Authorized list from the Administrator application. After adding the drive serial number you will not be notified again. Each partition has its own unique serial number so make sure you add each one. You should also check mark the "Don't Log this drive" so these drives are not written to the approved log every time you start the PC.
3. If any computer loses network connection to the server ALL USB drives will be ejected unless you have activated cached mode. This prevents someone from trying to circumvent this software by simply disconnecting the network connection. Since the database would not be able to be contacted everything gets ejected when the network connection is lost even approved drives. Cached mode writes all approved drives to each workstation so when its off your network it can still allow these drives. Restart the pc if approved drives have changed and the pc is back on your network.
4. Certain USB devices such as some smart phones need to be mounted from the device itself before they are recognized by Windows. During this time there is no Serial number to be read even though there is a new drive letter showing up. Because the device has not been mounted the drive letter shows up in Windows, but cannot be opened. This application has a Timer mode and when this mode is activated by the administrator, the user who plugs in this type of device will have 15 seconds to mount the device. If they fail to do this in time the device will be ejected. If they do it in time then the serial number will be checked. Either way, the devices can still draw power from the USB port to charge its battery even if it is has been ejected.
5. Certain Computers have Multi-Card readers that have many different card slots for reading different types of cards like SD, Compact Flash, Memory Stick etc. These types of devices all share the same connection to the computers motherboard. Hence, if one drive in the device is ejected, all of them get ejected at the same time. This is caused by slots which have no serial number. Drives that do not have a serial number are ejected. To prevent this type of device from being ejected every time the computer starts there is an option call "Allow Drives With No Serial Numbers From Certain PC's". You can find this option on the main Administrators window menu under "Options & Settings". After checking this option you must add the computers name on your network that has this type of device.
6. If you have a USB drive with encryption software that after entering a password unlocks another partition on that drive and creates another drive letter you must also authorize this addition drive or it will be ejected.
7. Some USB drives such as those with encryption software on them, install software on a PC that is activated and opens an application located on the USB device and locking it. If this type of software is already on the PC prior to installing USB Drive Guard the drive may not be ejected, but all others will be able to be ejected as normal. Lexar drives will be ejected because we have identified the exe process that is called. If you have a brand other than Lexar email us the exe name and we will include it in our next release.

- 8.** USB drive ejection software ejects unauthorized drives at two different times: When the garde.exe application starts, (when the computer starts, or when a user logs into their Windows account), and when it detects a new drive.
- 9.** We advise you to format a USB drive before approving it and giving it to your users. Formatting will ensure a unique serial number. Manufactures create batches of USB drives at a factory with the same serial number. So if you did not format the drive first and approved it, then if another person plugged in a similar model of USB drive then they could be allowed to use it because it has the same serial number as one of your other approved users.
- 10.** Our Support page has instructions on how to deploy this software with a GPO or similar systems.