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

**www.usbdriveguard.com**

**Contact Email: 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 Windows.

You can download the newest version from the website **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.

## Installation Steps:

The file USBDriveFullSetup.exe is installed one PC used as the server, and is the only installer needed.

**Server Installation:** First you must make sure that your Server PC has a static IP address. An IP that doesn't change since the software will contact to the database by IP address.

To install Start the setup file called USBDriveFullSetup.exe you just downloaded and choose all the default settings during installation. All database setting are setup automatically. You will install this onto just **one** PC on your network this will be your Server. You do not have to install on a version of Windows "Server". Any modern version of Windows will do for the Administrator Server application.

The default user name and password when logging into the USB Drive Guard Administrator application, "USBAdmin.exe", is "admin" for both. You should change the password as soon as you can for security purposes. This will be the only installation that you need to perform. The ejection client software is deployed after you scan your network with the "USBAdmin.exe" application that is on the server that you installed in this step

**Work Station Client Installation:** Workstation ejection clients are pushed and installed from the Server installed app called "USBsetup.exe" that you just installed with the USBDriveFullSetup.exe file above. Run this application from the Server and scan your network and right click the workstation name and choose Deploy Ejection Client

**Database Backups:** www.usbdriveguard.com/downloads/usbdriveguard/MySQL/Backup-Silent.exe

If you want to do backups you can run the above Backup-Silent.exe on the MySQL server pc as a scheduled task. This will create an sql backup file in the same folder that the Backup-Silent.exe is located.

**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 service starts, 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.