



Notes: USB Levels of security settings:

Advanced Systems has years of experience working with company's helping them secure and control the usability of removable USB memory devices. We understand that there are three levels a USB can be stopped. To assist you in locating the product that will best fit your needs I would like to offer our opinion in hopes that it will be of help in some way in your efforts.

These levels in order based on strength of protection are:

I) BIOS MACHINE LEVEL:

Strongest but with limitations that in today's increase use of USB devices makes this a unrealistic method. The three major problems encountered when attempting to use this method are.

- It will block the use of non storage USB peripherals on the machine.
- Can not be managed remotely.
- Requires physically restart machine to make changes.

II) Operating System Level

The strongest level with the flexibility to accomplish control yet be usable in real work environment. This is the level we used when developing USB Lock RP.

- Allows non-storage peripherals to work.
- Allows the management of the ports remotely.
- Restarting the operating system is not required.

III) User Level

This is the weakest level of control, providing a very limited level of security.

- The device has already entered the system. Code from the device can be executed from the allowed user session. This code can be designed to jump a session.
- User Level often relies on "Read Only" which represents limited to no protection against an execution.
- By only marking an executable read only you can double click on it and it will still work.
- System remains open to malicious software code that will not require that it be installed by an administrator and who knows what instructions it will have.