



Technical FAQ

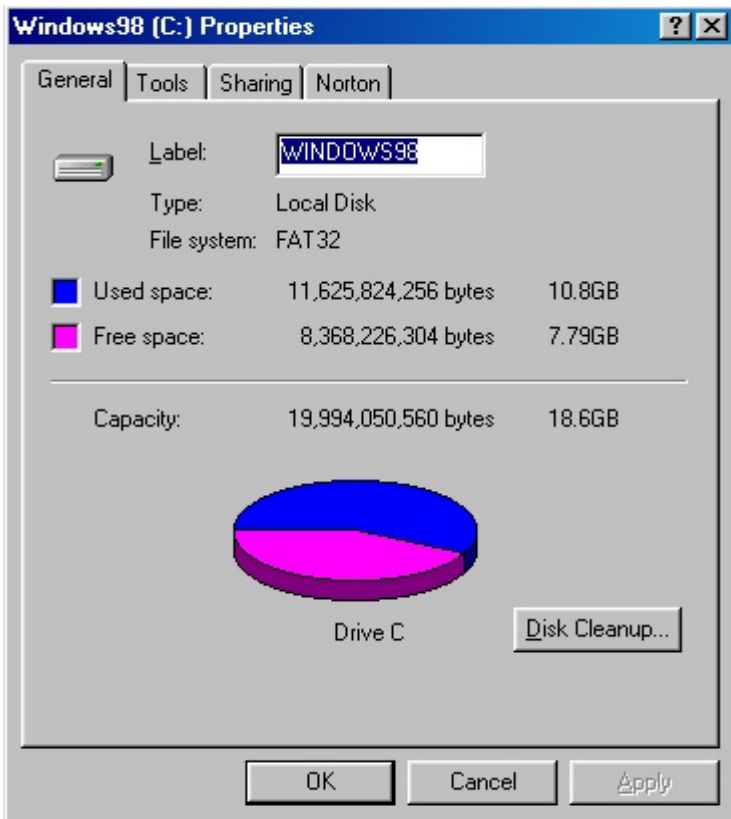
This document is intended to provide detailed technical information on how the HardGuard protects the computer hard drive. It should be emphasized that it is not necessary for a user to understand this information in order to use HardGuard. Instead, this information is intended to satisfy the curiosity of the more technical user.

BIOS EXTENSION - HardGuard works as an extension of the PC BIOS. Specifically, HardGuard changes the way you read/write data on a hard drive. The BIOS modification can be described as a File Allocation Table redirector. This BIOS extension is realized when the system boots from the HardGuard instead of the hard drive. Therefore, it is mandatory that the PC motherboard supports booting from a Network Boot ROM. This capability is supported on the vast majority of motherboards, as the specification has been part of the published PC BIOS since the introduction of the Token Ring card in the early 1980's. The open architecture philosophy promoted by IBM allows us to produce products such as the HardGuard. On the rare occasion that you find a system without Network Boot ROM support, that PC does not truly meet the definition of an IBM compatible PC!

INSTALL PROCESS - When the HardGuard card is installed, several things happen. First, the HardGuard takes ownership of the first 2 cylinders of the hard drive (cylinder 0 and 1). This space usually contains the "boot strap" of the Microsoft operating system. This boot strap is copied to the next available set of cylinders on the hard drive. The HardGuard then modifies the Master Boot Record of the hard drive to point to the new cylinder location for the boot strap.

The first 2 cylinders are now available for the HardGuard to store key information about the system. This includes the CMOS settings, the supervisor password, and other key pieces of information about the hard drive telemetry. It is important to note that all the information about the system is stored on the hard disk drive. No information about the system is stored on the card. All the memory on the card is dedicated to implementing the protection methodology.

Now the HardGuard takes inventory of the hard drive, making a record of which sectors contain data, and which sectors are available as free space on the hard drive. The free space is the area that will be used by the HardGuard to control any attempts to modify the original data on the hard drive.



This is how Windows typically presents the properties of a hard disk drive. Some users find it helpful to think of the space on the hard drive as slices from a pie.

For illustration purposes, let's pretend that the file "AUTOEXEC.BAT" is located on this hard drive in Cylinder 4, Sector 1. We can call this C4S1.

When the system is directed to "read" the AUTOEXEC, the BIOS asks the HardGuard where the file is located. The HardGuard will respond with the address of the file (C4S1).

When the user attempts to change the AUTOEXEC, the "write" request is sent to the HardGuard. The HardGuard will not

allow this change to C4S1 to occur. Instead, the HardGuard sends the new data to a sector in the "free space". Let's pretend that HardGuard found Cylinder 24, Sector 19 (C24S19) as the next available free space.

The next time the user attempts to read the AUTOEXEC, the HardGuard tells the system to go to C24S19 for the data. The original data in C4S1 is never changed. HardGuard keeps a record of all the changed information on the hard drive. Depending upon the HardGuard Mode setting, this record of changes is handled differently.

AUTO MODE - the change record is discarded every time the PC is booted. When the PC is booted, the system will be told to use C4S1 for the AUTOEXEC.

SAVE, RESTORE, TIMER - The record of changes is kept between boots. The system will continue to point to C24S19 for the AUTOEXEC until a "restore" of the hard drive is initiated. On the other hand, if the owner decides to "save" the changed image, the HardGuard will make the new location permanent. After the save, the original space on the hard drive (C4S1) is now considered free space.

INSTALL MODE - All changes are immediately accepted as part of the permanent image. HardGuard does not keep any record of the changes, therefore there is no way to undo any changes that are made in this mode. This is how a PC normally operates.

DISASTER RECOVERY - In the unlikely event that a HardGuard card is damaged or stolen, a new card can be placed in the system. It is not necessary to uninstall the card. This is possible because no system specific information is stored on the card. All of the necessary information is stored on the hard drive (Sectors 0 and 1 are for the system CMOS and password, the file change records are stored in a protected area in the free space on the hard drive).

If the user makes any changes to the system while the card is removed, it is important to realize that the changes will probably cause the operating system and applications to fail. This is because the changes will be made regardless of the HardGuard's record of the file location. When the card is put back in the system, the HardGuard will try to point the user to the old location for a file. It is very possible that this data has been replaced when the user modified the system without the HardGuard installed.

If a system hard drive is compromised in this fashion, it will be necessary to perform a low level format of the hard drive (be sure to include sector 0 and 1). This will purge the HardGuard record of changes to the system. This type of low level formatting generally requires a special program that is provided by the hard drive manufacturer. You should be sure to remove the HardGuard card before you attempt this type of maintenance.