



## Using Trash Guard

When you enable Trash Guard, all deleted files, even ones you delete in DOS or in 16-bit applications, are moved to the Recycle Bin. When you start the Trash Guard application, you enable it.

**Tip** We recommend that you activate Trash Guard so it always runs when you run Windows. By running Trash Guard, you ensure that you can recover files you've deleted later if you discover that you need them.

These topics explain how to use Trash Guard:

- ❑ [Starting Trash Guard](#)
- ❑ [Selecting Trash Guard Properties](#)
- ❑ [Disabling Trash Guard](#)
- ❑ [Adding the Nuts & Bolts Tab to the Recycle Bin's Properties Sheet](#)
- ❑ [Excluding Files from Trash Guard's Delete Protection](#)

---

### Related Topics

[Nuts & Bolts Contents](#)

## Starting Trash Guard

When you start Trash Guard, you activate it.

**Tip** If you have added Trash Guard's Nuts & Bolts tab in the Recycle Bin's Properties sheet, you can also Right-click the Recycle Bin icon in My Computer or Windows Explorer, choose Properties, select the Nuts & Bolts tab, and select the Enable Trash Guard check box.

### To start Trash Guard:

1. Start Trash Guard by doing one of the following:

- ▣ Click the Start button and choose the Program > Nuts & Bolts > Trash Guard command in Windows 95.

- ▣ Open the Nuts & Bolts folder and double-click the Trash Guard icon from the Windows 95 Explorer or My Computer window.

The Trash Guard dialog box appears.

2. Click OK.

Trash Guard remains active until you decide to disable it.

## Selecting Trash Guard Properties

Trash Guard's Properties sheet lets you decide if the Trash Guard Properties tab (the tab titled Nuts & Bolts) appears in the Recycle Bin's Properties sheet dialog box. You can also specify any files to exclude from delete protection.

### To select Trash Guard properties:

1. Start Trash Guard by doing one of the following:
  - ❑ Click the Start button and choose the Program > Nuts & Bolts > Trash Guard command in Windows 95.
  - ❑ Open the Nuts & Bolts folder and double-click the Trash Guard icon from the Windows 95 Explorer or My Computer window.

The Trash Guard dialog box appears.

2. Click the Properties button.

The Trash Guard Properties dialog box appears.

3. Select the options you want to use.

4. Do one of the following:



Click the Apply button when you finish selecting options so you can continue making other selections.



Click OK when you finish selecting properties.

The Trash Guard dialog box reappears.

## Disabling Trash Guard

You can disable Trash Guard whenever you like.

### To disable Trash Guard:

1. Start Trash Guard by doing one of the following:



Click the Start button and choose the Program > Nuts & Bolts > Trash Guard command in Windows 95.



Open the Nuts & Bolts folder and double-click the Trash Guard icon from the Windows 95 Explorer or My Computer window.

The Trash Guard dialog box appears.

2. Click the Disable button.

Trash Guard asks you to confirm that you want to disable delete protection.

3. Click Yes.

Trash Guard closes, is disabled and the desktop reappears.

**Tip** If Trash Guard's Properties tab is available in the Recycle Bin's Properties sheet, you can also disable Trash Guard by Right-clicking the Recycle Bin icon in My Computer or Windows Explorer, choosing Properties, selecting the Nuts & Bolts tab, and deselecting the Enable Trash Guard check box.

## Adding the Nuts & Bolts Tab to the Recycle Bin's Properties Sheet

You can decide whether you want Trash Guard's Properties tab (labeled Nuts & Bolts) to be available in the Recycle Bin's Properties sheet.

### To add the Nuts & Bolts tab to the Recycle Bin's Properties sheet:

1. Start Trash Guard by doing one of the following:



Click the Start button and choose the Program > Nuts & Bolts > Trash Guard command in Windows 95.



Open the Nuts & Bolts folder and double-click the Trash Guard icon from the Windows 95 Explorer or My Computer window.

The Trash Guard dialog box appears.

2. Click the Properties button.

The Trash Guard Properties dialog box appears.

3. Deselect the Hide Recycle Bin Properties Tab check box.
4. Click OK.

The Trash Guard dialog box reappears.

5. Click OK.

## Excluding Files From Trash Guard's Delete Protection

You can add files to the list of files to exclude from Trash Guard's delete protection. After you've added files, you can also modify their path or remove them from the list.

### To exclude files from Trash Guard's delete protection:

1. Start Trash Guard by doing one of the following:



Click the Start button and choose the Program > Nuts & Bolts > Trash Guard command in Windows 95.



Open the Nuts & Bolts folder and double-click the Trash Guard icon from the Windows 95 Explorer or My Computer window.

The Trash Guard dialog box appears.

2. Click the Properties button.

The Trash Guard Properties dialog box appears.

3. Click the Add New button.

4. Locate the files to exclude from delete protection or the path to a folder or directory of files to exclude.

Trash Guard also lets you select files in the Files To Exclude list and click Modify to modify the definition of these files, or click the Remove button to remove them from the list of files to exclude.

You can use standard wildcard characters to exclude all files that have the same file extension or similar names. The wildcard characters you can use are:



**Asterisk ( \* )**-a multiple-character placeholder. For example if you enter \*.BAK, all files that have the .BAK file extension would be excluded from delete protection. Or if you enter ~\*.\*, all files that start with a tilde ( ~ ) and have any file extension would be excluded from delete protection.



**Question Mark ( ? )**-a single-character placeholder. For example, you could enter map??\*.bmp to exclude a range of files named map01.bmp through map99.bmp.

4. Do one of the following:



Click the Apply button when you finish selecting options so you can continue making other selections.



Click OK when you finish selecting properties.

The Trash Guard dialog box reappears.

5. Click OK.

## Trash Guard Dialog Box

This dialog box contains the following options:

### **Disable**

Click the Disable button to turn off Trash Guard. Trash Guard displays a confirmation message. Click Yes and Trash Guard closes and returns to the desktop.

### **Properties**

Click the Properties button to select the Trash Guard properties settings you want to use. The Trash Guard Properties dialog box appears.

### **OK**

Click the OK button to close Trash Guard.

## **Trash Guard Properties Dialog Box**

This dialog box contains the following options:

### **Enable Trash Guard**

Select this check box if you want to enable Trash Guard so that it protects the files you delete. Deselect this check box to turn off Trash Guard's delete protection.

### **Files to Exclude / Add New**

Click the Add New button and Trash Guard positions the cursor in the first empty line of the Files to Exclude list so you can specify a file or a directory of files to exclude from delete protection. Once you've added an entry to the Files to Exclude list, you can select it and then modify or remove it.

### **Modify**

Select an entry in the Files to Exclude list and click the Modify button to edit that entry.

### **Remove**

Select an entry in the Files to Exclude list and click the Remove button to remove that file from the Files to Exclude list.

### **OK**

Click OK when you are finished specifying Trash Guard properties.

### **Cancel**

Click Cancel to close the Trash Guard Properties dialog box without making any changes to the properties settings since the last time you clicked Apply. The Trash Guard dialog box reappears.

### **Apply**

Click Apply to apply any changes you've made in the Trash Guard tab.



## **Nuts & Bolts Properties Tab**

You can show or hide the Nuts & Bolts Properties tab that contains the same options as the Trash Guard Properties sheet dialog box in the Recycle Bin's Properties sheet.

## **Address Space**

The sum total of all possible memory addresses available at a given time. This is 4 GB (gigabytes) on a 386 or later PC in protected mode.

## **Launch Pad**

The Launch Pad is a window where you can place application and document icons so you can conveniently access them.

## **Benchmarks**

A benchmark is a standardized task that tests various devices for measurements, such as speed.

## **BIOS**

The BIOS (or Basic Input/Output System) contains buffers for sending information from an application to the hardware device, such as a printer, where the information should go.

## **Buffers**

A buffer is a temporary storage location for information being sent or received.

## **Bytes**

A byte is eight bits of information composed of zeros and ones, one of which may be a parity bit. Most character sets, such as ASCII, use one byte to represent each character (letter, number, or special symbol).

## **Cache**

A cache is part of the computers memory used to temporarily store recently accessed information. A cache is designed on the premise that recently used information may be needed again soon. Keeping information available in cache reduces the time it takes for an application to obtain the information again.



**Cluster**

A cluster is a unit of storage allocation usually consisting of four or more 512-byte sectors.

## **Conventional Memory**

Conventional memory is the first 640 K (kilobytes) of RAM (random access memory).

## **CPU (Central Processing Unit)**

The brain of your computer. This is main computer chip that controls all activity that takes place on a computer.

## **Diagnostics**

Diagnostics are tests run to detect faults in a computer system. Diagnostics tests are run to detect faults before they become serious problems so the faults can be corrected.

## **Directories**

Directories are locations within a volume on a drive where you can store files or subdirectories. In Windows 95, directories are equivalent to folders that appear on the desktop in a drive window.

## **Discardable Memory**

Discardable memory is memory used by an application that it has marked as discardable. Windows can reallocate the discardable memory to a different application if it needs to.

## **DLLs (Dynamic Link Libraries)**

A DLL is an executable code module that can be loaded on demand and linked at run time. DLLs can be shared among multiple applications and independently updated, transparent to the applications. DLLs can also be unloaded when they are no longer needed.

**DMA (Direct Memory Access)**

DMA is a fast method of moving information from a storage device or LAN interface card directly to RAM which speeds processing time. DMA is direct memory access by a peripheral device that by-passes the CPU to save time.



## **Expanded Memory**

DOS running on the Intel 80286, 80386, or 80486 family of computers can only address one megabyte of memory at one time. Expanded memory is the memory located between the base memory (either 512 K or 640 K) and one megabyte. Expanded memory is reserved by DOS for housekeeping tasks, such as managing information that appears on the screen.

## **Extended Memory**

Memory above one megabyte in 80286 and higher PCs. Extended memory can be used for RAM disks, disk caches, or Windows, but it requires the CPU to run in a special mode (protected mode or virtual real mode).

## **FAT (File Allocation Table)**

The FAT is a roadmap, or index, that points to the location where all the information in files is stored on a floppy disk or hard drive. The FAT is extremely important because the system uses it to store and retrieve files containing information.

When you save a file in Windows, it is stored in multiple pieces (in clusters made up of multiple sectors) on the disk. Windows also saves the roadmap, or index, that points to these clusters in two copies of the FAT (File Allocation Table). The FAT contains the directions to all the pieces of your files, so that applications can find them again later.

## **GDT (General Description Table)**

The GDT is a table that is basic to the operation of protected mode. This table contains data structures (descriptors) that describe various regions of memory and how they may be accessed. Windows uses the GDT for system devices. See [LDT](#).

## **Global Heap**

The Global Heap is the general pool of memory available to Windows applications.

**GPF (General Protection Fault)**

An error condition caused by an application when it attempts to perform an operation not allowed by the operating system. Windows uses GPFs to determine and control the state of the currently executing application. GPFs that are unexpected by Windows cause a system error message to appear.

## **HMA (High Memory Area)**

The HMA is the first 64 K of extended memory. If you use DOS 5.0, you can save memory by loading DOS into the HMA. Do this by adding the DOS=HIGH setting to your CONFIG.SYS file and restarting your PC.

## **Interrupt**

A temporary suspension of a process caused by an event outside that process. More specifically, an interrupt is a signal or call to a specific routine. Interrupts allow peripheral devices, such as printers or modems, to send a call to the CPU requesting attention.



## **I/O (Input/Output) Device**

An I/O device is any piece of computer hardware that can exchange information with the CPU. Examples of I/O devices include network cards, printers, speakers or other sound devices, or devices connected to the serial or parallel ports of your PC such as external modems.

## **Kernel**

The Kernel is the part of a computer operating system that performs basic functions such as switching between tasks.

## **LDT (Local Descriptor Table)**

The LDT is a secondary data structure table that contains additional information about various regions of memory and how they can be accessed. Windows uses the LDT for programs.

## **Linear Memory**

Linear memory is the currently defined address space of the system that Windows uses to allocate memory to Windows applications.

## **Local Heap**

The Local Heap is a region of memory allocated for local use by an application.

## **Locked Memory**

Locked memory is memory used by an application that cannot be relocated or discarded by Windows.

## **Mapping**

Mapping is the process of assigning physical memory (RAM) to a particular linear address range.

## **Mode Switch**

A mode switch is a transition made by the CPU when changing from one mode of operation to another. For example, switching from real or protected mode, or a transition between different levels of protection. See [Ring 0, 1, 2, 3](#).



## **Modules**

A module is a device driver loaded by Windows.

## **Paging**

The process of saving information stored in RAM to the swap file on the system hard drive so Windows can make the RAM available at a different linear address.

## **Parallel Port**

The parallel port is a connector on the back of your PC and on some peripheral devices. With the appropriate driver software installed and a parallel cable connected to the parallel ports on your PC and a peripheral device, the two can communicate with each other. Parallel transmissions have no EIA standard, but most equipment follows a quasi-standard called the Centronics Parallel Standard.

## **PCI (Peripheral Component Interconnect) Bus**

The PCI Bus is a local motherboard specification (that provides connector slots on the motherboard for installing peripheral cards). The PCI Bus, designed by Intel, offers a high performance, peripheral component level interface to the CPU bus.

## **Physical Memory**

Physical memory is the RAM (Random Access Memory) installed in your PC. See [Random Access Memory \(RAM\)](#).

**Protected Mode**

A mode of operation of 80286 or later CPUs which allows access to more than 1 MB of memory.

## **RAM (Random Access Memory)**

RAM (Random Access Memory) is also called physical memory. It is installed in your PC on SIMMs (Single Inline Memory Modules) or DIMMs (Dual Inline Memory Modules). RAM is volatile, extremely high-speed storage used by your computer for processing information.

## **Real Mode**

A mode of 80286 or later CPUs, where the CPU operates substantially like an older 8086 CPU and can address directly only 1 MB of memory.



## **Resources**

Resources are objects that Windows and its applications can use, such as the buttons on the screen that you can click.

## **Ring 0, 1, 2, 3**

Different levels of protection in protected mode, where programs having varying degrees of freedom of operation. Ring 0 (zero) is least protected and has direct access to all hardware in the system.

**Sector**

A sector is a pie-shaped portion of a hard disk. A disk is divided into tracks and sectors. Tracks are complete circuits and are divided into sectors. Under DOS, a sector is 512 bytes.

## **Serial Port**

A serial port is an input/output port (connector) that allows the transmission of information out at one bit at a time, as opposed to parallel which transmits eight bits, or one byte at a time.

## **Swap File**

The swap file is created by Windows on the system hard disk. It uses the swap file to copy information stored in part of the linear address space so it can reallocate the RAM used at that location to another linear address space.

## **Swapping**

Swapping is the process of saving to disk or restoring from disk the contents of RAM so that the RAM can be used elsewhere in linear memory.

## System Resources

System resources are a series of data structures kept by Windows. System resources are managed by the Windows User and GDI programs and maintain information about objects that appear on your screen. For instance, for each button on your screen the User program has to know where it is supposed to be located, what program owns it, and which part of the program needs to be notified when you click the button. GDI must maintain information about pens used to draw lines on screen, fonts used to draw characters, and so on.

The information about the various objects managed by the User and GDI programs is kept in six 64K regions of memory known as resource heaps. These regions are actually 64K local heaps. These regions are 64K because 64K is the maximum size a 16-bit program can deal with efficiently. User and GDI are 16-bit programs because Windows was originally designed to run on the Intel 8088 and 80286, 16-bit processors.

The User Resource Heaps are divided into:



The Window Heap, which contains information on windows and controls



The Menu Heap, which contains information on drop-down menus



The Menu String Heap, which contains the text messages that appear in the menus



The User Atom Heap, which contains mostly Window titles

The GDI Resource Heaps are:



The main GDI Resource Heap, which contains pens, brushes, fonts and various other information related to displaying Graphics



The GDI Atom Heap, which contains some font related information including font names.

The GDI and User Atom Heaps are usually discounted because the information in them is subsidiary to the other Local Resource Heaps. So, the other Heaps would always fill up before the Atom Heaps. The same is still true if Hurricane's Heap Expander (another Helix Software product) is loaded, although all the Heaps have been greatly expanded (now you understand the "Heap Expander" name too).

### **32BDA (32-Bit Disk Access)**

32BDA is a process in Windows where the device driver that accesses the disk runs entirely as a 32-bit program at Ring 0 (zero).



### **32BFA (32-Bit File Access)**

32BFA is a process in Windows where the DOS file operations are controlled by a program, or set of devices, that operate entirely as 32-bit programs at Ring 0 (zero).

## **Unlocked Memory**

Unlocked memory is physical memory that Windows can copy to the swap file on disk, and whose linear address can be changed whenever Windows chooses.

**UMB (Upper Memory Block)**

The UMB is the area in memory between 640 K and 1 MB that have RAM mapped into them by memory managers, such as Helix Netroom or MemMaker. See [Expanded memory](#).

## **V86 Mode (Virtual 8086 Mode)**

V86 mode is a mode of operation of 80386 or later CPUs where programs, originally designed to run in real mode, can run as sub-programs to a protected mode control program or operating system.

## **Video Memory**

Video memory, called VRAM, is physical memory installed on your PC's video card that is used for displaying information on the screen.

## **Virtual Memory**

Virtual memory is the amount of memory that exists either as physical memory (RAM) or on the hard drive (in the swap file). When a part of memory that is located in the swap file is accessed by an application, Windows reads the information into RAM.

## **VMs (Virtual Machines)**

Virtual machines (also called Virtual DOS machines or VDMs) are created in Windows 95 when you open a MS-DOS Prompt window. The VDM is a software emulation of a separate computer, offering all the services that the DOS application expects of a PC.

## **VxDs (Virtual Device Drivers)**

VxDs are used in Windows 95 to communicate with all physical hardware in the system. This prevents any application from having direct access to a piece of hardware. Instead, it communicates only through the VxD for that hardware.



## **Windows 95 Registry**

The Windows 95 Registry file contains user, application, and computer-specific configuration information in a central location that was kept in various .INI files in Windows 3.1. The Registry contains settings that determine how your computer runs.

## Hidden Files

A hidden file is any file that does not show up in a regular directory listing. Typically, hidden files have one of the following file extensions:



DLL-(Dynamic Link Library)



SYS-System file



VXD-Virtual Device Driver



386-Virtual Device Driver



DRV-Device Driver

In Windows, a programmer can set any file with the hidden file attribute.

**Tip** In Windows Explorer or My Computer, you can select to show or hide hidden files. To do this, choose the Options command from the View menu, click the View tab, select the Show or the Hide radio button, and click OK.

## **System Files**

A system file is a file used exclusively by the operating system, or Windows.

